Maths 4 Number Theory Notes 2012

Chris Smyth, University of Edinburgh
c.smyth @ ed.ac.uk

0. Reference books

There are no books I know of that contain all the material of the course. however, there are many texts on Number Theory in the library. Here are a small selection of them.

- Course in p-adic analysis by Alain M. Robert, Springer GTM 2000.
  Library: QA241 Rob.
- A friendly introduction to number theory by J. H. Silverman, Prentice Hall, 2001.
  QA241 Sil
- Introduction to the theory of numbers by G.H. Hardy and E.M. Wright.
  QA241 Har.
- Introduction to the theory of numbers by Ivan Niven and Herbert S. Zuckerman.
  QA241 Niv.
- Introduction to number theory by Lo-keng Hua Springer-Verlag, 1982.
  QA241 Hua

1. The integer part (= floor) function

Definition 1. For $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the *floor*, or *integer part* of x. It is defined as the largest integer $\leq x$.

So we have $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. The graph of $\lfloor x \rfloor$ is a 'staircase' function, constant on $[n, n+1)$ and a jump of 1 at n, for each $n \in \mathbb{Z}$.

Note that for $x > 0$, $\lfloor x \rfloor$ is the number of positive integers $\leq x$. Alternative notation is $[x]$. It looks like a trivial function, but it satisfies some surprising identities (as well as some not-so-surprising ones!)

Proposition 1.1. *For $x \in \mathbb{R}$ and $n \in \mathbb{N}$ we have*

(i) $\lfloor k + x \rfloor = k + \lfloor x \rfloor$ *for* $k \in \mathbb{Z}$, $x \in \mathbb{R}$.
(ii) $\left\lfloor \frac{\ell}{n} + \delta \right\rfloor = \left\lfloor \frac{\ell}{n} \right\rfloor$ *for* $\ell \in \mathbb{N}$ *and* $0 \leq \delta < \frac{1}{n}$.
(iii)

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor .$$

Proof. (i) and (ii) are easy. For (iii), note that if it is true for x then, using (i), it is true for $x + k$, $k \in \mathbb{Z}$ (k is added to both sides), so we can assume that $0 \leq x < 1$.

Now write $x = \frac{\ell}{n} + \delta$ $(0 \le \delta < \frac{1}{n})$ for ℓ/n the largest rational with denominator n that is $\le x$. Then $0 \le \ell < n$ and for $j = 0, 1, \ldots, n-1$

$$\begin{aligned}\left\lfloor x + \frac{j}{n} \right\rfloor &= \left\lfloor \frac{\ell}{n} + \delta + \frac{j}{n} \right\rfloor \\ &= \left\lfloor \frac{\ell + j}{n} \right\rfloor \qquad \text{(using (ii))} \\ &= \begin{cases} 1 \text{ if } j \ge n - \ell; \\ 0 \text{ otherwise.} \end{cases}\end{aligned}$$

So the LHS of (iii) sums to ℓ. But its RHS is $\lfloor nx \rfloor = \lfloor \ell + n\delta \rfloor = \ell$, as $n\delta < 1$. Hence RHS=LHS. □

Proposition 1.2. *Let $r_1, \ldots, r_k \in \mathbb{R}$. Then*

$$\sum_{i=1}^{k} \lfloor r_i \rfloor \le \left\lfloor \sum_{i=1}^{k} r_i \right\rfloor \le \sum_{i=1}^{k} \lfloor r_i \rfloor + k - 1.$$

Proof. If it's true for all $r_i \in [0, 1)$ then it's true for all r_i (just add an integer N to some r_i, which adds N to $\lfloor r_i \rfloor$ and N to $\left\lfloor \sum_{i=1}^{k} r_i \right\rfloor$. Do this for each i.). So we can assume that all $r_i \in [0, 1)$, giving all $\lfloor r_i \rfloor = 0$ and $0 \le \sum_{i=1}^{k} r_i < k$ and hence $0 \le \left\lfloor \sum_{i=1}^{k} r_i \right\rfloor \le k - 1$. □

These two inequalities are both best possible of their type, since the left one has equality when all the r_i are integers, and the right one has equality when all the r_i are in $[\frac{k-1}{k}, 1)$.

Corollary 1.3. *Let $n = n_1 + \cdots + n_k$, where the n_i are in $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Then the multinomial coefficient*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! n_2! \ldots n_k!} = B$$

say, is an integer.

Proof. From Problem Sheet 1, Q8(a) we know that for each prime p the power of p that divides $n!$ is $\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$, a finite sum. So the power of p dividing B is

$$\begin{aligned}\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor - \sum_{i=1}^{k} \sum_{j=1}^{\infty} \left\lfloor \frac{n_i}{p^j} \right\rfloor &= \sum_{j=1}^{\infty} \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \sum_{i=1}^{k} \left\lfloor \frac{n_i}{p^j} \right\rfloor \right) \\ &\ge 0,\end{aligned}$$

by the above Proposition, on putting $r_i = n_i/p^j$. Thus B is divisible by a nonnegative power of p for every prime p, so must be an integer. □

Another way to prove that this number is an integer is to show that it is the coefficient of $x_1^{n_1} \ldots x_k^{n_k}$ in the expansion of $(x_1 + \cdots + x_k)^n$.

Say that $p, q \in \mathbb{N}$ are *coprime* (or *relatively prime*) if $\gcd(p, q) = 1$.

Proposition 1.4. *Let p and q be two coprime odd positive integers. Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

We shall see later that this result will be used in the proof of the Law of Quadratic Reciprocity.

Proof. Consider the rectangle with corners $(0,0)$, $(p/2,0)$, $(0,q/2)$ and $(p/2,q/2)$. (Suggest you draw it, along with its diagonal from $(0,0)$ to $(p/2,q/2)$, and the horizontal axis the k-axis, the vertical axis the ℓ-axis. The diagonal is then the line with equation $\ell = kq/p$.) We count the number of integer lattice points (k,ℓ) strictly inside this rectangle in two different ways. First we note that these points form a rectangle with corners

$$(1,1), (\frac{p-1}{2}, 1), (1, \frac{q-1}{2}), (\frac{p-1}{2}, \frac{q-1}{2}),$$

so that there are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ of them in all.

On the other hand, we count separately those below and above the diagonal. Below the diagonal we have, for $k = 1, \ldots \frac{p-1}{2}$ that $\left\lfloor \frac{kq}{p} \right\rfloor$ is the number of points (k,ℓ) with $1 \le \ell \le \frac{kq}{p}$, i.e., below the diagonal, in the kth column. So the total is $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$.

To count the number of lattice points above the diagonal, we flip the diagram over, reversing the rôles of p and q, and of k and ℓ. Then we get that the number of points above the diagonal is $\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor$. It remains to check that there are no lattice points actually *on* the diagonal. For if the integer lattice point (k,ℓ) were on the diagonal $\ell = kq/p$ we would have $\ell p = kq$ so that, as p and q are coprime, $p \mid k$. But $k < p$, so this is impossible. □

As an exercise, can you state and prove the variant of this result in the case that p and q, while still odd, need not be coprime?

One should also be aware of the following variants of $\lfloor x \rfloor$:

- The *ceiling of* x, $\lceil x \rceil$, is the least integer $\ge x$. Note that $\lceil x \rceil = -\lfloor -x \rfloor$.
- The *nearest integer to* x (no standard notation) can be defined either as $\lfloor x + \frac{1}{2} \rfloor$, where then the nearest integer to $\frac{1}{2}$ is 1, or as $\lceil x - \frac{1}{2} \rceil$, where then the nearest integer to $\frac{1}{2}$ is 0.

2. Congruences

Recall that $x \equiv a \pmod{m}$ means that $m \mid (x-a)$, or that $x = a + km$ for some $k \in \mathbb{Z}$. Recall too that if $a, b \in \mathbb{Z}$ then there are $a', b' \in \mathbb{Z}$ such that $aa' + bb' = \gcd(a,b)$. The numbers a', b' can be found using the Extended Euclidean Algorithm, which you may recall from your First Year. In particular, when $\gcd(a,b) = 1$ there are $a', b' \in \mathbb{Z}$ such that $aa' + bb' = 1$. Then $aa' \equiv 1 \pmod{b}$, so that a' is the inverse of $a \pmod{b}$.

2.1. **Chinese Remainder Theorem.**

Theorem 2.1 (Chinese Remainder Theorem)**.** *Given $m_1, \ldots, m_k \in \mathbb{N}$ with $\gcd(m_i, m_j) = 1 \quad (i \neq j)$ ("pairwise coprime"), and $a_1, \ldots, a_k \in \mathbb{Z}$, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a solution $x \in \mathbb{Z}$.

Proof. In fact x can be constructed explicitly. For $i = 1, \ldots, k$ define m_i' to be the inverse $(\mathrm{mod}\ m_i)$ of $m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$, so that

$$m_1 \ldots m_{i-1} m_i' m_{i+1} \ldots m_k \equiv 1 \pmod{m_i}.$$

Then $x = \sum_{i=1}^{k} a_i m_1 \ldots m_{i-1} m_i' m_{i+1} \ldots m_k \equiv a_i \pmod{m_i}$ for $i = 1, \ldots, k$, because every term except the ith is divisible by m_i. □

Then, if x_0 is one solution to this set of congruences, it's easy to see (how?) that the general solution is $x = x_0 + \ell m_1 \cdots m_k$ for any integer ℓ. In particular, there is always a choice of ℓ giving a unique solution x in the range $0 \leq x < m_1 \cdots m_k$ of the set of congruences.

Q. If the m_i not pairwise coprime, what is the condition on the a_i's so that the set of congruences above again has a solution x?

One answer: factorize each m_i as a product of prime powers:

$$m_i = \prod_j p_j^{r_{ji}},$$

where the p_j's are the prime factors of $\prod_i m_i$, and the r_{ji} are all ≥ 0. Then replace the congruence $x \equiv a_i \pmod{m_i}$ by the set of congruences $x \equiv a_i \pmod{p_j^{r_{ji}}}$ for each j (justify!). Next, collect together all the congruences whose modulus is a power of the same prime, say (changing notation!) $x \equiv a_1 \pmod{p^{n_1}}, \ldots, x \equiv a_\ell \pmod{p^{n_\ell}}$. Then if these congruences are pairwise consistent, we need only take the one with the largest modulus (p^{n_ℓ} say). So we end up taking just one congruence for each p, and so the moduli we take are all pairwise coprime. (Two congruences $x \equiv a_1 \pmod{p^m}$ and $x \equiv a_2 \pmod{p^n}$ with $m \leq n$ (note: same p in both) are *pairwise consistent* if $a_2 \equiv a_1 \pmod{p^m}$.) If some such pair of congruences are not consistent, then that pair of congruences, and hence the original set of congruences, has no solution.

An example of an inconsistent pair of congruences is $x \equiv 0 \pmod{2}$, $x \equiv 1 \pmod{4}$.

Lemma 2.2. (i) *The congruence $ax \equiv b \pmod{m}$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(a, m) \mid b$; in this case the number of solutions x is $\gcd(a, m)$.*

(ii) *If $x^a \equiv 1 \pmod{m}$ and $x^b \equiv 1 \pmod{m}$ then $x^{\gcd(a,b)} \equiv 1 \pmod{m}$.*

Proof. (i) Put $g = \gcd(a, m)$. Then $b = ax + km$ shows that $g \mid b$. Conversely, if $g \mid b$ then $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$ and $\gcd(\frac{a}{g}, \frac{m}{g}) = 1$ (justify!). So $\frac{a}{g}$ has an inverse $\pmod{\frac{m}{g}}$ and $x \equiv \frac{b}{g} \cdot \left(\frac{a}{g}\right)^{-1} \pmod{\frac{m}{g}}$.

The g different solutions to $ax \equiv b \pmod{m}$ are then $x_0 + k\frac{m}{g}$ for $k = 0, 1, \ldots, g-1$, for any solution x_0 of $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$.

(ii) We have $\gcd(a, b) = aa' + bb'$ say, by the Extended Euclidean algorithm, so

$$x^{\gcd(a,b)} = x^{aa'+bb'} = (x^a)^{a'} \cdot (x^b)^{b'} \equiv 1 \pmod{m}.$$

□

2.2. **Solving equations in $\mathbb{F}_p$.** We now restrict our congruences to a prime modulus p, and consider the solutions of equations $f(x) = 0$ for $f(x) \in \mathbb{F}_p[x]$ and $x \in \mathbb{F}_p$. Since $\mathbb{F}_p = \mathbb{Z}/(p)$, this is equivalent, for $f(x) \in \mathbb{Z}[x]$, of solving $f(x) \equiv 0 \pmod{p}$ for $x \in \{0, 1, 2, \ldots, p-1\}$.

Theorem 2.3. *A nonzero polynomial $f \in \mathbb{F}_p[x]$ of degree n has at most n roots x in $\mathbb{F}_p$.*

Proof. Use induction: for $n = 1$, $f(x) = ax + b$ say, with $a \neq 0$, whence $f(x) = 0$ has a solution $x = a^{-1}b$ in $\mathbb{F}_p$.

Now assume $n \geq 1$ and that the result holds for n. Take $f(x) \in \mathbb{F}_p[x]$ of degree $n + 1$. If $f = 0$ has no roots $x \in \mathbb{F}_p$ the the result is certainly true. Otherwise, suppose $f(b) = 0$ for some $b \in \mathbb{F}_p$. Now divide $x - b$ into $f(x)$, (i.e., one step of the Euclidean algorithm for polynomials) to get $f(x) = (x - b)f_1(x) + r$ say, where f_1 is of degree n, and $r \in \mathbb{F}_p$. Putting $x = b$ shows that $r = 0$. Hence $f(x) = (x-b)f_1(x)$, where f_1 has, by the induction hypothesis, at most n roots $x \in \mathbb{F}_p$. So f has at most $n + 1$ roots $x \in \mathbb{F}_p$, namely b and those of $f_1 = 0$. Hence the result is true for $n + 1$ and so, by induction, true for all $n \geq 1$. □

Note that the proof, and hence the result, holds equally well when $\mathbb{F}_p$ is replaced by *any* field F. However, it does not hold when the coefficients of f lie in a ring with zero divisors. For instance, on replacing F by the ring $\mathbb{Z}/8\mathbb{Z}$, the equation $x^2 - 1 \equiv 0 \pmod{8}$ has *four* solutions $x = 1, 3, 5, 7 \pmod{8}$.

Question. Where in the above proof was the fact that we were working over a field used?

2.3. **$\mathbb{F}_p^\times$ is cyclic!** Denote by $\mathbb{F}_p^\times$ the multiplicative group $\mathbb{F}_p \setminus \{0\}$, using the field multiplication (and forgetting about its addition).

We need some group theory at this stage. Recall that the *exponent* of a finite group G is the least $e \in \mathbb{N}$ such that $g^e = 1$ for each $g \in G$.

Let C_r denote the cyclic group with r elements: $C_r = \{1, g, g^2, \ldots, g^{r-1} \mid g^r = 1\}$. Here

Proposition 2.4. *Let G be a finite abelian group with $\#G$ elements. If G is noncyclic then its exponent is $< \#G$.*

Proof. For the proof, recall the Fundamental Theorem of Abelian Groups, which tells us that any such G is isomorphic to a product

$$C_{n_1} \times C_{n_2} \times C_{n_3} \times \cdots \times C_{n_{k-1}} \times C_{n_k}$$

of cyclic groups, for some $k \in \mathbb{N}$ and integers $n_1, \ldots, n_k$ all > 1 and such that $n_1 \mid n_2$, $n_2 \mid n_3, \ldots, n_{k-1} \mid n_k$. Hence all n_i's divide n_k and so n_k is the exponent of G. However, $\#G = n_1 n_2 \ldots n_k$, which is greater than n_k as $k > 1$. □

Proposition 2.5. *For p an odd prime, the group $\mathbb{F}_p^\times$ is cyclic (of size $p-1$ of course).*

Proof. Suppose $\mathbb{F}_p^\times$ were noncyclic. Then, by the previous Proposition, there would exist an exponent $e < p-1$ such that $x^e = 1$ for each $x \in \mathbb{F}_p^\times$. But then the equation $x^e = 1$ would have more than e solutions in $\mathbb{F}_p$, contradicting Theorem 2.3. □

A generator g of the cyclic group $\mathbb{F}_p^\times$ (p an odd prime) is called a *primitive root* $\pmod p$. Then we can write $\mathbb{F}_p^\times = \langle g \rangle$.

2.4. **Number of primitive roots.** Given a prime p, how many possible choices are there for a generator g of $\mathbb{F}_p^\times$? To answer this, we need to define Euler's φ-function. Given a positive integer n, $\varphi(n)$ is defined as the cardinality of the set $\{k : 1 \le k \le n \text{ and } \gcd(k,n) = 1\}$.

So for instance $\varphi(1) = 1$, $\varphi(6) = 2$ and $\varphi(p) = p-1$ for p prime.

Proposition 2.6. *For p an odd prime, there are $\varphi(p-1)$ primitive roots* $\pmod p$.

Proof. Take one primitive root g. Then g^k is again a primitive root iff $(g^k)^\ell = g$ in $\mathbb{F}_p^\times$ for some ℓ, i.e., $g^{k\ell - 1} = 1$. But $g^n = 1$ iff $(p-1) \mid n$. So g^k is a primitive root iff $k\ell - 1 \equiv 0 \pmod{p-1}$. This is impossible (why?) if $\gcd(k, p-1) > 1$, while if $\gcd(k, p-1) = 1$ then the extended Euclidean algorithm will give us ℓ. □

2.5. **Quadratic residues and nonresidues.** Take p an odd prime, and $r \in \mathbb{F}_p^\times$. If the equation $x^2 = r$ has a solution $x \in \mathbb{F}_p^\times$ then r is called a *quadratic residue* $\pmod p$. If there is no such solution x, then r is called a *quadratic nonresidue* $\pmod p$.

Proposition 2.7. *Take p an odd prime, and g a primitive root* $\pmod p$. *Then the quadratic residues* $\pmod p$ *are the even powers of g, while the quadratic nonresidues* $\pmod p$ *are the odd powers of g. (So there are $\frac{p-1}{2}$ of each.)*

In particular, $\left(\frac{g^k}{p}\right) = (-1)^k$.

Proof. Suppose $r \in \mathbb{F}_p^\times$, with $r = g^k$ say. If k is even then $r = (g^{k/2})^2$, so that r is a quadratic residue $\pmod p$. Conversely, if $x = g^\ell$, $x^2 = r$, then $g^{2\ell - k} = 1$, so that $2\ell - k$ is a multiple of $p-1$, which is even. So k is even. □

2.6. **The Legendre symbol.** Let p be an odd prime, and $r \in \mathbb{F}_p^\times$. Then the *Legendre symbol* is defined as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 \text{ if } r \text{ is a quadratic residue;} \\ -1 \text{ if } r \text{ is a quadratic nonresidue.} \end{cases}$$

Note that, on putting $r = g^k$ we see that

$$\left(\frac{g^k}{p}\right) = (-1)^k = \begin{cases} 1 \text{ if } k \text{ is even;} \\ -1 \text{ if } k \text{ is odd.} \end{cases}$$

Next, recall Fermat's Theorem: that $r^{p-1} = 1$ for all $r \in \mathbb{F}_p^\times$. This is simply a consequence of $\mathbb{F}_p^\times$ being a group of size (order) $p-1$. (We know that $g^{\#G} = 1$ for each g in a finite group G.)

Proposition 2.8 (Euler's Criterion)**.** *For p an odd prime and $r \in \mathbb{F}_p^\times$ we have in $\mathbb{F}_p^\times$ that*

$$\left(\frac{r}{p}\right) = r^{\frac{p-1}{2}}. \tag{1}$$

Proof. If $r = g^k$ then for k even

$$r^{\frac{p-1}{2}} = g^{k\frac{p-1}{2}} = (g^{p-1})^{k/2} = 1^{k/2} = 1,$$

while if k is odd, $k\frac{p-1}{2}$ is not a multiple of $p-1$, so $r^{\frac{p-1}{2}} \neq 1$. However, $r^{p-1} = 1$ by Fermat, so $r^{\frac{p-1}{2}} = \pm 1$ and hence $r^{\frac{p-1}{2}} = -1$. So, by Proposition 2.7, we have (1), as required. □

In particular ($r = -1$), for p an odd prime, we have

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Lemma 2.9. *Let p be an odd prime, and a, b be integers not divisible by p. We have*

(1) *$a \equiv b \pmod p$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;*
(2) *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;*
(3) *$\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.*

Proof. Let g be a primitive root $\pmod p$. Then $\left(\frac{g^k}{p}\right) = (-1)^k$, from which the results follow easily. □

2.7. **Taking nth roots in $\mathbb{F}_p^\times$.** Take an odd prime p and g a fixed primitive root $\pmod p$. Then for any $B \in \mathbb{F}_p^\times$ we define the *index* (old-fashioned word) or *discrete logarithm* (current jargon) of B, written $\operatorname{ind} B$ or $\log_p B$, as the integer $b \in \{0, 1, \ldots, p-2\}$ such that $B = g^b$ in $\mathbb{F}_p$. Clearly the function $\log_p$ depends not only on p but also on the choice of the primitive root g.

Proposition 2.10. *Given $n \in \mathbb{N}$ and $B \in \mathbb{F}_p^\times$, the equation $X^n = B$ in $\mathbb{F}_p^\times$ has a solution $X \in \mathbb{F}_p^\times$ iff $\gcd(n, p-1) \mid \log_p B$.*

When $\gcd(n, p-1) \mid \log_p B$ then the number of distinct solutions X of $X^n = B$ in $\mathbb{F}_p^\times$ is $\gcd(n, p-1)$.

Proof. Write $B = g^b$, $X = g^x$, so that $g^{nx} = g^b$, giving $nx \equiv b \pmod{p-1}$. Now apply Lemma 2.2(i) to this congruence. □

For large primes p, the problem of finding the discrete logarithm $\log_p B$ of B appears to be an intractable problem, called the *Discrete Logarithm Problem*. Many techniques in Cryptography depend on this supposed fact. See e.g.,

`http://en.wikipedia.org/wiki/Discrete_logarithm`

3. Arithmetic functions

3.1. **Arithmetic functions.** These are functions $f : \mathbb{N} \to \mathbb{N}$ or $\mathbb{Z}$ or maybe $\mathbb{C}$, usually having some arithmetic significance. An important subclass of such functions are the multiplicative functions: such an f is *multiplicative* if

$$f(nn') = f(n)f(n')$$

for all $n, n' \in \mathbb{N}$ with n and n' coprime ($\gcd(n, n') = 1$).

Proposition 3.1. *If f is multiplicative and $n_1, \dots, n_k$ are pairwise coprime ($\gcd(n_i, n_j) = 1$ for all $i \neq j$) then*

$$f(n_1 n_2 \dots n_k) = f(n_1)f(n_2)\dots f(n_k).$$

This is readily proved by induction.

Corollary 3.2. *If n factorises into distinct prime powers as $n = p_1^{e_1} \dots p_k^{e_k}$ then*

$$f(n) = f(p_1^{e_1}) \dots f(p_k^{e_k}).$$

So multiplicative functions are completely determined by their values on prime powers. Some examples of multiplicative functions are

- The '1-detecting' function $\Delta(n)$, equal to 1 at $n = 1$ and 0 elsewhere – obviously multiplicative;
- $\tau(n) = \sum_{d|n} 1$, the number of divisors of n;
- $\sigma(n) = \sum_{d|n} d$, the sum of the divisors of n.

Proposition 3.3. *The functions $\tau(n)$ and $\sigma(n)$ are both multiplicative.*

Proof. Take n and n' coprime, with $\ell_1, \dots, \ell_{\tau(n)}$ the divisors of n, and $\ell'_1, \dots, \ell'_{\tau(n')}$ the divisors of n'. Then all the $\tau(n)\tau(n')$ numbers $\ell_i \ell'_j$ are all divisors of nn'. Conversely, if m divides nn' then $m = \ell\ell'$, where $\ell \mid n$ and $\ell' \mid n'$. (Write m as a product of prime powers, and then ℓ will be the product of the prime powers where the prime divides n, while ℓ' will be the product of the prime powers where the prime divides n'. Note that n and n', being coprime, have no prime factors in common.) So ℓ is some ℓ_i and ℓ' is some ℓ'_j, so all factors of nn' are of the form $\ell_i \ell'_j$. Thus $\tau(nn') = \tau(n)\tau(n')$, and

$$\sigma(nn') = \sum_{i,j} \ell_i \ell'_j = \left(\sum_i \ell_j\right)\left(\sum_j \ell'_j\right) = \sigma(n)\sigma(n').$$

□

Given an arithmetic function f, define its 'sum over divisors' function $F(n) = \sum_{d|n} f(d)$.

Proposition 3.4. *If f is multiplicative, and $n = \prod_p p^{e_p}$ then*

$$F(n) = \prod_{p|n} \left(1 + f(p) + f(p^2) + \cdots + f(p^{e_p})\right). \tag{2}$$

Further, F is also multiplicative.

Proof. Expanding the RHS of (2), a typical term is $\prod_{p|n} f(p^{e'_p})$, where $0 \le e'_p \le e_p$. But, by the multiplicivity of f, this is simply $f(d)$, where $d = \prod_{d|n} p^{e'_p}$ is a divisor of n. Conversely, every divisor of n is of this form, for some choice of exponents e'_p. Hence the RHS of (2) is equal to $\sum_{d|n} f(d)$, which is $F(n)$.

Next, taking n and n' coprime, we see that (2) immediately implies that $F(n)F(n') = F(nn')$, i.e., that F is multiplicative. □

Proposition 3.5. *Euler's φ-function $\varphi(m)$ is multiplicative.*

Proof. Take n and n' coprime, and let

$$\{i : 1 \le i \le n, \gcd(i, n) = 1\} = \{a_1 < a_2 < \cdots < a_{\varphi(n)}\},$$

the *reduced residue classes* $\bmod n$. Similarly, let

$$\{j : 1 \le j \le n', \gcd(j, n') = 1\} = \{a'_1 < a'_2 < \cdots < a'_{\varphi(n')}\}.$$

If $x \in \{1, 2, \ldots, nn'\}$ and $\gcd(x, nn') = 1$ then certainly $\gcd(x, n) = \gcd(x, n') = 1$, so that

$$x \equiv a_i \pmod{n} \qquad x \equiv a'_j \pmod{n'} \tag{3}$$

for some pair a_i, a'_j. Conversely, given such a pair a_i, a'_j we can solve (3) using the CRT to get a solution $x \in \{1, 2, \ldots, nn'\}$ with $\gcd(x, nn') = 1$. Thus we have a bijection between such x and such pairs a_i, a'_j. Hence

$$\#\{\text{such } x\} = \varphi(nn') = \#\{a_i, a'_j\} = \varphi(n)\varphi(n').$$

□

In passing, mention

Proposition 3.6 (Euler's Theorem)**.** *If $a, n \in \mathbb{N}$ and $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. This is because the reduced residue classes $\bmod n$ form a multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of size(order) $\varphi(n)$. So, in this group, $a^{\varphi(n)} = 1$. □

Note that on putting $n = p$ prime we retrieve Fermat's Little Theorem $a^{p-1} \equiv 1 \pmod{p}$.

[In fact the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is usually smaller than $\varphi(n)$. To give the exponent, we need to define a new function ψ on prime powers by $\psi = \varphi$ on odd prime

powers, and at 2 and 4, while $\psi(2^e) = \frac{1}{2}\varphi(2^e)$ if $e \geq 3$. Then the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\mathrm{lcm}_{p:p^{e_p}||n}\, \psi(p^{e_p})$. This follows from the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{p:p^{e_p}||n} (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$$

and the fact that $(\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$ has exponent $\psi(p^{e_p})$.]

Proposition 3.7. *We have* $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$.

Proof. Now $\varphi(p^k) = p^k - p^{k-1}$ (why?), which $= p^k\left(1 - \frac{1}{p}\right)$, so the result follows from Corollary 3.2. □

The *Möbius function* $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 0 \text{ if } p^2 \mid n \text{ for some prime } p; \\ (-1)^k \text{ if } n = p_1 p_2 \dots p_k \text{ for distinct primes } p_i. \end{cases}$$

In particular, $\mu(1) = 1$ and $\mu(p) = -1$ for a prime p. It is immediate from the definition that μ is multiplicative. Then, applying (2), we see that $\sum_{d|n}\mu(d) = \Delta(n)$.

Integers with $\mu(n) = \pm 1$ are called *squarefree*.

The Möbius function arises in many kinds of *inversion* formulae. The fundamental one is the following.

Proposition 3.8 (Möbius inversion)**.** *If* $F(n) = \sum_{d|n} f(d) \quad (n \in \mathbb{N})$ *then for all* $n \in \mathbb{N}$ *we have* $f(n) = \sum_{d|n}\mu(n/d)F(d)$.

Proof. Simplify $\sum_{d|n}\mu(n/d)F(d) = \sum_{d|n}\mu(n/d)\sum_{k|d} f(k) \quad (n \in \mathbb{N})$ by interchanging the order of summation to make $\sum_{k|n}$ the outer sum. But a simpler proof is given below. □

3.2. **Dirichlet series.** For an arithmetic function f, define its *Dirichlet series* $D_f(s)$ by

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Here $s \in \mathbb{C}$ is a parameter. Typically, such series converge for $\Re s > 1$, and can be meromorphically continued to the whole complex plane. However, we will not be concerned with analytic properties of Dirichlet series here, but will regard them only as generating functions for arithmetic functions, and will manipulate them formally, without regard to convergence.

The most important example is for $f(n) = 1 \quad (n \in \mathbb{N})$, which gives the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$. Also, taking $f(n) = n \quad (n \in \mathbb{N})$ gives $\zeta(s-1)$. (Check!).

Proposition 3.9. *If* f *is multiplicative then*

$$D_f(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots + \frac{f(p^k)}{p^{ks}} + \dots\right) = \prod_p D_{f,p}(s), \tag{4}$$

say.

Proof. Expanding the RHS of (4), a typical term is

$$\frac{f(p_1^{e_1})f(p_2^{e_2})\dots f(p_r^{e_r})}{p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}} = \frac{f(n)}{n^s}$$

for $n = \prod_{i=1}^r p_i^{e_i}$, using the fact that f is multiplicative. □

Such a product formula $D_f(s) = \prod_p D_{f,p}(s)$ over all primes p is called an *Euler product* for $D_f(s)$.

For example

$$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots + \frac{1}{p^{ks}} + \dots\right) = \prod_p \left(\frac{1}{1-p^{-s}}\right),$$

on summing the Geometric Progression (GP). Hence also

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - p^{-s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = D_\mu(s),$$

on expanding out the product.

Proposition 3.10. *We have*

$$\left(\sum_k \frac{a_k}{k^s}\right) \cdot \left(\sum_\ell \frac{b_\ell}{\ell^s}\right) = \left(\sum_n \frac{c_n}{n^s}\right),$$

where $c_n = \sum_{k|n} a_k b_{n/k}$.

Proof. On multiplying out the LHS, a typical term is

$$\frac{a_k}{k^s} \cdot \frac{b_\ell}{\ell^s} = \frac{a_k b_{n/k}}{n^s},$$

where $k\ell = n$. So all pairs k, ℓ with $k\ell = n$ contribute to the numerator of the term with denominator n^s. □

Corollary 3.11. *We have* $D_F(s) = D_f(s)\zeta(s)$.

Proof. Apply the Proposition with $a_k = f(k)$ and $b_\ell = 1$. □

Corollary 3.12 (Möbius inversion again)**.** *We have* $f(n) = \sum_{d|n} \mu(n/d)F(d)$ *for all* $n \in \mathbb{N}$.

Proof. From Corollary 3.11 we have

$$D_f(s) = D_F(s) \cdot \frac{1}{\zeta(s)} = \left(\sum_k \frac{F(k)}{k^s}\right) \cdot \left(\sum_\ell \frac{\mu(\ell)}{\ell^s}\right) = \left(\sum_n \frac{c_n}{n^s}\right),$$

where $c_n = \sum_{k|n} F(k)\mu(n/k)$. But $D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, so, on comparing coefficients, $f(n) = \sum_{k|n} F(k)\mu(n/k)$. □

We now compute the Dirichlet series for a few standard functions. [Part (a) is already proved above.]

Proposition 3.13. *We have*

(a) $D_\mu(s) = \frac{1}{\zeta(s)}$;
(b) $D_\varphi(s) = \frac{\zeta(s-1)}{\zeta(s)}$;
(c) $D_\tau(s) = \zeta(s)^2$;
(d) $D_\sigma(s) = \zeta(s-1)\zeta(s)$.

Proof. (b) Now

$$\begin{aligned} D_\varphi(s) &= \prod_p \left(1 + \frac{\varphi(p)}{p^s} + \frac{\varphi(p^2)}{p^{2s}} + \cdots + \frac{\varphi(p^k)}{p^{ks}} + \dots\right) \\ &= \prod_p \left(1 + \frac{p-1}{p^s} + \frac{p^2-p}{p^{2s}} + \cdots + \frac{p^k - p^{k-1}}{p^{ks}} + \dots\right) \\ &= \prod_p \left(1 + \frac{p-1}{p^s} \cdot \frac{1}{1-p^{1-s}}\right), \qquad \text{on summing the GP} \\ &= \prod_p \left(\frac{1-p^{-s}}{1-p^{-(s-1)}}\right), \qquad \text{on simplification} \\ &= \frac{\zeta(s-1)}{\zeta(s)}. \end{aligned}$$

(c) Now

$$\begin{aligned} D_\tau(s) &= \prod_p \left(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \cdots + \frac{\tau(p^k)}{p^{ks}} + \dots\right) \\ &= \prod_p \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \cdots + \frac{k+1}{p^{ks}} + \dots\right) \\ &= \prod_p \frac{1}{(1-p^{-s})^2} \qquad \text{using } (1-x)^{-2} = \sum_{k=0}^{\infty} (k+1)x^k \\ &= \zeta(s)^2 \end{aligned}$$

(d) This can be done by the same method as (b) or (c) – a good exercise! But, given that we know the answer, we can work backwards more quickly:

$$\zeta(s-1)\zeta(s) = \left(\sum_k \frac{k}{k^s}\right) \cdot \left(\sum_\ell \frac{1}{\ell^s}\right) = \sum_n \frac{\sum_{k|n} k \cdot 1}{n^s} = D_\sigma(s),$$

using Prop. 3.10

□

3.3. **Perfect numbers.** A positive integer n is called *perfect* if it is the sum of its proper (i.e., excluding n itself) divisors. Thus $\sigma(n) = 2n$ for n perfect.

Proposition 3.14. *An even number n is perfect iff it of the form $n = 2^{p-1}(2^p - 1)$ for some prime p with the property that $2^p - 1$ is also prime.*

Prime numbers of the form $2^p - 1$ are called *Mersenne primes*. (Unsolved problem: are there infinitely many such primes?)

It is easy to check that $\sigma(2^{p-1}(2^p - 1)) = 2^p(2^p - 1)$ when $2^p - 1$ is prime. The converse is more difficult — I leave this as a tricky exercise: you need to show that if $k \geq 2$ and $2^{k-1}p_1 \dots p_\ell$ is perfect then $\ell = 1$ and $p_1 = 2^k - 1$. (It's easy to prove that if $2^k - 1$ is prime then so is k.)

It is an unsolved problem as to whether there are any odd perfect numbers. See e.g., `http://en.wikipedia.org/wiki/Perfect_number` for lots on this problem.

4. Primality testing

4.1. **Introduction.** Factorisation is concerned with the problem of developing efficient algorithms to express a given positive integer $n > 1$ as a product of powers of distinct primes. With primality testing, however, the goal is more modest: given n, decide whether or not it is prime. If n does turn out to be prime, then of course you've (trivially) factorised it, but if you show that it is not prime (i.e., *composite*), then in general you have learnt nothing about its factorisation (apart from the fact that it's not a prime!).

One way of testing a number n for primality is the following: suppose a certain theorem, Theorem X say, whose statement depends on a number n, is true when n is prime. Then if Theorem X is false for a particular n, then n cannot be prime. For instance, we know (Fermat) that $a^{n-1} \equiv 1 \pmod{n}$ when n is prime and $n \nmid a$. So if for such an a we have $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime. This test is called the *Pseudoprime Test to base a*. Moreover, a composite number n that passes this test is called a *Pseudoprime to base a*.

(It would be good if we could find a Theorem Y that was true *iff* n was prime, and was moreover easy to test. Then we would know that if the theorem was true for n then n was prime. A result of this type is the following (also on a problem sheet): n is prime iff $a^{n-1} \equiv 1 \pmod{n}$ for $a = 1, 2, \dots, n-1$. This is, however, not easy to test; it is certainly no easier than testing whether n is divisible by a for $a = 1, \dots, n$.)

4.2. **Proving primality of n when $n-1$ can be factored.** In general, primality tests can only tell you that a number n either 'is composite', or 'can't tell'. They cannot confirm that n is prime. However, under the special circumstance that we can factor $n-1$, primality can be proved:

Theorem 4.1 (Lucas Test, as strengthened by Kraitchik and Lehmer)**.** *Let $n > 1$ have the property that for every prime factor q of $n-1$ there is an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ but $a^{(n-1)/q} \not\equiv 1 \pmod{n}$. Then n is prime.*

Proof. Define the subgroup G of $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the subgroup generated by all such a's. Clearly the exponent of G is a divisor of $n-1$. But it can't be a proper divisor of $n-1$, for then it would divide some $(n-1)/q$ say, which is impossible as $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for the a corresponding to that q. Hence G has exponent $n-1$. But then

$n-1 \leq \#G \leq \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$. Hence $\varphi(n) = n-1$, which immediately implies that n is prime. □

Corollary 4.2 (Pepin's Test, 1877)**.** *Let $F_k = 2^{2^k}+1$, the kth Fermat number, where $k \geq 1$. Then F_k is prime iff $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$.*

Proof. First suppose that $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$. We apply the theorem with $n = F_k$. So $n-1 = 2^{2^k}$ and $q = 2$ only, with $a = 3$. Then $3^{\frac{F_k-1}{2}} \not\equiv 1 \pmod{F_k}$ and (on squaring) $3^{F_k-1} \equiv 1 \pmod{F_k}$, so all the conditions of the Theorem are satisfied.

Conversely, suppose that F_k is prime. Then, by Euler's criterion and quadratic reciprocity (see Chapter 5) we have

$$3^{\frac{F_k-1}{2}} \equiv \left(\frac{3}{F_k}\right) = \left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

as 2 is not a square $\pmod 3$.

□

We can use this to show that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are all prime. It is known that F_k is composite for $5 \leq k \leq 32$, although complete factorisations of F_k are known only for $0 \leq k \leq 11$, and there are no known factors of F_k for $k = 20$ or 24. Heuristics suggest that there may be no more k's for which F_k is prime.

4.3. **Carmichael numbers.** A *Carmichael number* is a (composite) number n that is a pseudoprime to every base a with $1 \leq a \leq n$ and $\gcd(a,n) = 1$. Since it it immediate that $a^{n-1} \not\equiv 1 \pmod n$ when $\gcd(a,n) > 1$, we see that Carmichael numbers are pseudoprimes to as many possible bases as any composite number could be. They are named after the US mathematician Robert Carmichael (1879 – 1967).

[But even *finding* an a with $\gcd(a,n) > 1$ gives you a factor of n. (Imagine that n is around 10^{300} and is a product of three 100-digit primes – such a's are going to be few and far between!)]

For examples of Carmichael numbers, see problem sheet 3.

4.4. **Strong pseudoprimes.** Given $n > 1$ odd and an a such that $a^{n-1} \equiv 1 \pmod n$, factorise $n-1$ as $n-1 = 2^f q$, where q is odd, $f \geq 1$ and consider the sequence

$$\mathcal{S} = [a^q, a^{2q}, a^{4q}, \ldots, a^{2^f q} \equiv 1],$$

taken $\pmod n$. If n is prime then, working left to right, either $a^q \equiv 1 \pmod n$, in which case $\mathcal{S}$ consists entirely of 1's, or the number before the first 1 must be -1. This is because the number following any x in the sequence is x^2, so if $x^2 \equiv 1 \pmod n$ for n prime, then $x \equiv \pm 1 \pmod n$. (Why?) A composite number n that has this property, (i.e., is a pseudoprime to base a and for which either $\mathcal{S}$ consists entirely of 1's or the number before the first 1 in $\mathcal{S}$ is -1) is called a *strong pseudoprime to base a*.

Clearly, if n is a prime or pseudoprime but not a strong pseudoprime, then this stronger test proves that n isn't prime. This is called the *Miller-Rabin Strong Pseudoprime Test.*

Perhaps surprisingly:

Theorem 4.3. *If n is a pseudoprime to base a but not a strong pseudoprime to base a, with say $a^{2^t q} \equiv 1 \pmod{n}$ but $a^{2^{t-1}q} \not\equiv \pm 1 \pmod{n}$, then n factors nontrivially as $n = g_1 g_2$, where $g_1 = \gcd(a^{2^{t-1}q} - 1, n)$ and $g_2 = \gcd(a^{2^{t-1}q} + 1, n)$.*

Proof. For then we have, for $n - 1 = 2^f q$ and some $t \le f$, that $a^{2^t q} \equiv 1 \pmod{n}$ but $a^{2^{t-1}q} \not\equiv \pm 1 \pmod{n}$. Now $a^{2^t q} - 1 = AB \equiv 0 \pmod{n}$, where $A = (a^{2^{t-1}q} - 1)$ and $B = (a^{2^{t-1}q} + 1)$, and neither A nor B is divisible by n. Hence g_1 is a nontrivial ($\neq 1$ or n) factor of n. Since $g_1 \mid n$, we have

$$\gcd(g_1, g_2) = \gcd(n, g_1, g_2) = \gcd(n, g_1, g_2 - g_1) = \gcd(n, g_1, 2) = 1,$$

the last step because n is odd. Hence any prime dividing n can divide at most one of g_1 and g_2. So from $n = \prod_p p^{e_p}$, say, and $n \mid AB$, we see that each prime power p^{e_p} dividing n divides precisely one of A or B, and so divides precisely one of g_1 or g_2. Hence $g_1 g_2 = n$. □

Example. Take $n = 31621$, a pseudoprime to base $a = 2$. We have $n - 1 = 2^2 \cdot 7905$, $2^{7905} \equiv 31313 \pmod{n}$ and $2^{15810} \equiv 2^{31620} \equiv 1 \pmod{n}$, so n is not a strong pseudoprime to base 2. Then $g_1 = \gcd(n, 31312) = 103$ and $g_2 = \gcd(n, 31314) = 307$, giving $n = 103 \cdot 307$.

Note that if $n = n_1 n_2$ where n_1 and n_2 are coprime integers, then by the Chinese Remainder Theorem we can solve each of the four sets of equations

$$x \equiv \pm 1 \pmod{n_1} \qquad\qquad x \equiv \pm 1 \pmod{n_2}$$

to get four distinct solutions of $x^2 \equiv 1 \pmod{n}$. For instance, for $n = 35$ get $x = \pm 1$ or ± 6. For the example $n = 31621$ above, we have $31313 \equiv 1 \pmod{103}$ and $31313 \equiv -1 \pmod{307}$, so that four distinct solutions of $x^2 \equiv 1 \pmod{31621}$ are ± 1 and ± 31313.

So what is happening when the strong pseudoprime test detects n as being composite is that some $x \in \mathcal{S}$ is a solution to $x^2 \equiv 1 \pmod{n}$ with $x \not\equiv \pm 1 \pmod{n}$ because $x \equiv 1 \pmod{n_1}$ and $x \equiv -1 \pmod{n_2}$ for some coprime n_1, n_2 with $n_1 n_2 = n$. And then both $\gcd(x - 1, n)$ (divisible by n_1) and $\gcd(x + 1, n)$ (divisible by n_2) are nontrivial factors of n.

4.5. **Strong pseudoprimes to the smallest prime bases.** It is known that

- 2047 is the smallest strong pseudoprime to base 2;
- 1373653 is the smallest strong pseudoprime to both bases 2, 3;
- 25326001 is the smallest strong pseudoprime to all bases 2, 3, 5;
- 3215031751 is the smallest strong pseudoprime to all bases 2, 3, 5, 7;
- 2152302898747 is the smallest strong pseudoprime to all bases 2, 3, 5, 7, 11;
- 3474749660383 is the smallest strong pseudoprime to all bases 2, 3, 5, 7, 11, 13;
- 341550071728321 is the smallest strong pseudoprime to all bases 2, 3, 5, 7, 11, 13, 17.

(In fact 341550071728321 is also a strong pseudoprime to base 19.)

Hence any odd $n < 341550071728321$ that passes the strong pseudoprime test for all bases 2, 3, 5, 7, 11, 13, 17 must be prime. So this provides a cast-iron primality test for all such n.

4.6. **Primality testing in 'polynomial time'.** In 2002 the Indian mathematicians Agrawal, Kayal and Saxena invented an algorithm, based on the study of the polynomial ring $(\mathbb{Z}/n\mathbb{Z})[x]$, that was able to decide whether a given n was prime in time $O((\log n)^{6+\varepsilon})$. (Here the constant implied by the 'O' depends on ε and so could go to infinity as $\varepsilon \to 0$.) (Search for 'AKS algorithm' on web.)

4.7. **The Lucas-Lehmer primality test for Mersenne numbers.** Given an odd prime p, let $M_p = 2^p - 1$, a *Mersenne number* (and a Mersenne prime iff it is prime). [It is an easy exercise to prove that if p is composite, then so is M_p.]

Define a sequence $S_1, S_2, \ldots, S_n, \ldots$ by $S_1 = 4$ and $S_{n+1} = S_n^2 - 2$ for $n = 1, 2, \ldots$. so we have

$$S_1 = 4, S_2 = 14, S_3 = 194, S_4 = 37634, S_5 = 1416317954, \ldots.$$

There is a very fast test for determining whether or not M_p is prime.

Theorem 4.4 (Lucas-Lehmer Test)**.** *For an odd prime p, the Mersenne number M_p is prime iff M_p divides S_{p-1}.*

So $M_3 = 7$ is prime as $7 \mid S_2$, $M_5 = 31$ is prime as $31 \mid S_4$,.... In this way get M_p prime for $p = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, \ldots$ (47th) 43112609. There may be others between the 41st and 47th. [as at October 2012.]

For the proof, we need two lemmas.

Lemma 4.5. *Put $\omega = 2 + \sqrt{3}$ and $\omega_1 = 2 - \sqrt{3}$. Then $\omega\omega_1 = 1$ (immediate) and*

$$S_n = \omega^{2^{n-1}} + \omega_1^{2^{n-1}}$$

for $n = 1, 2, \ldots$.

The proof is a very easy induction exercise.

Lemma 4.6. *Let r be a prime $\equiv 1 \pmod 3$ and $\equiv -1 \pmod 8$ (i.e., $\equiv 7 \pmod{24}$). Then*

$$\omega^{\frac{r+1}{2}} \equiv -1 \pmod r.$$

(So it's equal to $a + b\sqrt{3}$ where $a \equiv -1 \pmod r$ and $b \equiv 0 \pmod r$.)

Proof. Put

$$\tau = \frac{1+\sqrt{3}}{\sqrt{2}} \qquad \text{and} \qquad \tau_1 = \frac{1-\sqrt{3}}{\sqrt{2}}.$$

Then we immediately get $\tau\tau_1 = -1$, $\tau^2 = \omega$ and $\tau_1^2 = \omega_1$. Next, from $\tau\sqrt{2} = 1 + \sqrt{3}$ we have $(\tau\sqrt{2})^r = (1+\sqrt{3})^r$, so that

$$\begin{aligned}\tau^r 2^{\frac{r-1}{2}}\sqrt{2} &= 1 + \sum_{j=1}^{r-1}\binom{r}{j}(\sqrt{3})^j + 3^{\frac{r-1}{2}}\sqrt{3} \\ &\equiv 1 + 3^{\frac{r-1}{2}}\sqrt{3} \pmod{r}, \end{aligned} \tag{5}$$

as $r \mid \binom{r}{j}$. Since $r \equiv -1 \pmod 8$ we have

$$2^{\frac{r-1}{2}} \equiv \left(\frac{2}{r}\right) = (-1)^{\frac{r^2-1}{8}} \equiv 1 \pmod{r},$$

using Euler's Criterion, and Prop. 5.3. Further, since $r \equiv 1 \pmod 3$ and $r \equiv -1 \pmod 4$ we have

$$3^{\frac{r-1}{2}} \equiv \left(\frac{3}{r}\right) = \left(\frac{r}{3}\right)(-1)^{\frac{r-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{1}{3}\right)\cdot(-1) \equiv -1 \pmod{r},$$

using Euler's Criterion again, and also Quadratic Reciprocity (Th. 5.1). So, from (5), we have successively

$$\begin{aligned}\tau^r\sqrt{2} &\equiv 1 - \sqrt{3} \pmod r \\ \tau^r &\equiv \tau_1 \pmod r \\ \tau^{r+1} &\equiv \tau\tau_1 = -1 \pmod r \\ \omega^{\frac{r+1}{2}} &\equiv -1 \pmod r, \end{aligned}$$

the last step using $\tau^2 = \omega$. □

Proof of Theorem 4.4. **$\mathbf{M_p}$ prime $\Rightarrow$ $\mathbf{M_p \mid S_{p-1}}$.** Assume M_p prime. Apply Lemma 4.6 with $r = M_p$, which is allowed as $M_p \equiv -1 \pmod 8$ and $M_p \equiv (-1)^p - 1 \equiv 1 \pmod 3$. So

$$\omega^{\frac{M_p+1}{2}} = \omega^{2^{p-1}} \equiv -1 \pmod{M_p} \tag{6}$$

and, using Lemma 4.5, including $\omega_1^{-1} = \omega$, we have

$$S_{p-1} = \omega^{2^{p-2}} + \omega_1^{2^{p-2}} = \omega_1^{2^{p-2}}\left(\left(\omega_1^{-1}\right)^{2^{p-2}}\omega^{2^{p-2}} + 1\right) = \omega_1^{2^{p-2}}\left(\omega^{2^{p-1}} + 1\right) \equiv 0 \pmod{M_p}, \tag{7}$$

the last step using (6).

$\mathbf{M_p \mid S_{p-1}} \Rightarrow$ $\mathbf{M_p}$ prime. Assume $M_p \mid S_{p-1}$ but M_p composite. We aim for a contradiction. Then M_p will have a prime divisor q (say) with $q^2 \le M_p$.

Now consider the multiplicative group $G = \left(\frac{\mathbb{Z}[\sqrt{3}]}{(q)}\right)^\times$ of units of the ring $\frac{\mathbb{Z}[\sqrt{3}]}{(q)}$. Then G has coset representatives consisting of numbers $a + b\sqrt{3}$ with $a, b \in \{0, 1, 2, \ldots, q-1\}$ that are also invertible $\pmod q$. So G is a group of size (order) at most $q^2 - 1$, with multiplication defined modulo q. From $\omega(\omega_1 + q\sqrt{3}) \equiv 1 \pmod q$ we see that $\omega = 2 + \sqrt{3}$ is invertible, and so $\omega \in G$. [Strictly speaking, the coset $\omega \pmod q \in G$.]

Now, using $M_p \mid S_{p-1}$ we see that (7) holds even when M_p is composite, so we have successively that $\omega^{2^{p-1}} + 1 \equiv 0 \pmod{M_p}$, $\omega^{2^{p-1}} \equiv -1 \pmod{q}$ and $\omega^{2^p} \equiv 1 \pmod{q}$. Hence the order of ω in G is 2^p. Then $2^p \mid \#G \leq q^2 - 1 \leq M_p - 1 = 2^p - 2$, a contradiction. Hence M_p must be prime.

□

In practice, to test M_p for primality using Theorem 4.4, one doesn't need to compute $S_j (j = 1, 2, \ldots, p-1)$, but only the much smaller (though still large!) numbers $S_j \pmod{M_p} (j = 1, 2, \ldots, p-1)$.

A good source of information on Mersenne numbers is
`http://primes.utm.edu/mersenne/index.html`

5. Quadratic Reciprocity

5.1. **Introduction.** Recall that the Legendre symbol $\left(\frac{a}{p}\right)$ is defined for an odd prime p and integer a coprime to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue} \pmod{p}; \\ -1 \text{ otherwise;} \end{cases}$$

Recall too that for a, b coprime to p

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(easily proved by writing a, b as powers of a primitive root), and that, by Euler's Criterion,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv -1 \pmod{4}. \end{cases}$$

Theorem 5.1 (Law of Quadratic Reciprocity (Legendre, Gauss))**.** *For distinct odd primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

(Thus $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both $\equiv -1 \pmod{4}$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.)

There are now 240 recorded proofs of this (not all different), including six by Gauss – see
`http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`.

We'll give one of Gauss's proofs, using

Lemma 5.2 (Gauss's Lemma)**.** *For an odd prime p, put $p' = \frac{p-1}{2}$, and let a be an integer coprime to p. Consider the sequence*

$$a, 2a, 3a, ..., p'a,$$

reduced $\pmod p$ *to lie in* $(-\frac{p}{2}, \frac{p}{2})$. *Then* $\left(\frac{a}{p}\right) = (-1)^\nu$, *where* ν *is the number of negative numbers in this sequence.*

Proof. Now all of $a, 2a, 3a, ..., p'a$ are $\equiv \pmod p$ to one of $\pm 1, \pm 2, \ldots, \pm p'$. Further,

- no two are equal, as $ia \equiv ja \pmod p \Rightarrow i \equiv j \pmod p$;
- none is minus another, as $ia \equiv -ja \pmod p \Rightarrow i + j \equiv 0 \pmod p$.

So they must be $\pm 1, \pm 2, \ldots, \pm p'$, with each of $1, 2, \ldots, p'$ occurring with a *definite sign.* Hence

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot p'a \equiv (\pm 1) \cdot (\pm 2) \cdot \ldots \cdot (\pm p') \pmod p,$$

giving

$$a^{p'}(p')! \equiv (-1)^\nu (p')! \pmod p,$$

and so, as $(p')!$ is coprime to p, that

$$a^{p'} \equiv (-1)^\nu \pmod p.$$

Finally, using Euler's criterion (Prop. 2.8), we have

$$\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^\nu \pmod p.$$

Hence $\left(\frac{a}{p}\right) = (-1)^\nu$. □

We can use Gauss's Lemma to evaluate $\left(\frac{2}{p}\right)$.

Proposition 5.3. *For* p *an odd prime we have* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(This is equal to 1 when $p \equiv \pm 1 \pmod 8$, and to -1 when $p \equiv \pm 3 \pmod 8$.)

Proof. There are four similar cases, depending on $p \pmod 8$. We give the details for $p \equiv 3 \pmod 8$, $p = 8\ell + 3$ say. Then $p' = 4\ell + 1$, and, taking $a = 2$ in Gauss's Lemma, we see that for the sequence

$$2, 4, 6, \ldots, 4\ell, 4\ell + 2, \ldots, 8\ell + 2$$

that this becomes

$$2, 4, 6, \ldots, 4\ell, -(4\ell + 1), -(4\ell - 1), \ldots, -3, -1$$

when reduced $\pmod p$ into the range $(-\frac{p}{2}, \frac{p}{2})$. This clearly has 2ℓ positive members, and hence $\nu = p' - 2\ell = 2\ell + 1$ negative members. Hence $\left(\frac{2}{p}\right) = (-1)^{2\ell+1} = -1$. □

Doing the other three cases would be a good exercise!

We now use Gauss's Lemma with $a = q$ to prove the Law of Quadratic Reciprocity.

Proof of Theorem 5.1. Take distinct odd primes p and q. For $k = 1, 2, \ldots, p'$ write (one step of the Euclidean algorithm)

$$kq = q_k p + r_k \tag{8}$$

say, where $1 \leq r_k \leq p-1$ and

$$q_k = \left\lfloor \frac{kq}{p} \right\rfloor. \tag{9}$$

Now, working in $\mathbb{F}_p$ we have

$$\{q, 2q, \ldots, p'q\} = \{r_1, r_2, \ldots, r_{p'}\} = \{a_1, a_2, \ldots, a_t\} \cup \{-b_1, -b_2, \ldots, -b_\nu\},$$

as in Gauss's Lemma. So the a_i's are in $(0, \frac{p}{2})$ and the $-b_i$'s are in $(-\frac{p}{2}, 0)$. (In fact $t = p' - \nu$, but not needed.) Now put

$$a = \sum_{i=1}^{t} a_i, \qquad\qquad b = \sum_{i=1}^{\nu} b_i.$$

So, by the definition of the a_i's and $-b_i$'s we have

$$\sum_{k=1}^{p'} r_k = a - b + \nu p. \tag{10}$$

Now, in the proof of Gauss's Lemma we saw that

$$\{a_1, a_2, \ldots, a_t\} \cup \{b_1, b_2, \ldots, b_\nu\} = \{1, 2, \ldots, p'\},$$

so that

$$\frac{p^2-1}{8} = 1 + 2 + \cdots + p' = a + b. \tag{11}$$

and

$$\begin{aligned} \frac{p^2-1}{8} q &= \sum_{k=1}^{p'} kq \\ &= p \sum_{k=1}^{p'} q_k + \sum_{k=1}^{p'} r_k \qquad\qquad \text{(using (8))} \\ &= p \sum_{k=1}^{p'} q_k + a - b + \nu p, \qquad\qquad \text{(using (10).)} \end{aligned} \tag{12}$$

Next, on subtracting (12) from (11) we get

$$\frac{p^2-1}{8}(q-1) = p \sum_{k=1}^{p'} q_k - 2b + \nu p.$$

Reducing this modulo 2 we have $0 \equiv \sum_{k=1}^{p'} q_k - \nu \pmod 2$, or $\nu \equiv \sum_{k=1}^{p'} q_k \pmod 2$. Thus Gauss's Lemma gives

$$\left(\frac{q}{p}\right) = (-1)^{\nu} = (-1)^{\sum_{k=1}^{p'} q_k} = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor},$$

using (9).

Now, reversing the rôles of p and q we immediately get

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor},$$

where of course $q' = (q-1)/2$, and we've replaced the dummy variable k by ℓ. So

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left\{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor\right\}},$$

which equals $(-1)^{p'q'}$, by Prop. 1.4. □

6. Representation of integers as sums of two squares

Which $n \in \mathbb{Z}$ can be represented as a sum $n = x^2 + y^2$ for $x, y \in \mathbb{Z}$? Obviously need $n \geq 0$. Can clearly assume that x and y are nonnegative. We have $0 = 0^2 + 0^2$, $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, but no such representation for $n = 3$, 6 or 7.

Important note: $(2k)^2 \equiv 0 \pmod 4$, and $(2k+1)^2 = 8\binom{k+1}{2} + 1 \equiv 1 \pmod 8$ (and so certainly $\equiv 1 \pmod 4$).

6.1. The case $n = p$, prime.

Which primes are the sum of two squares?

Theorem 6.1. *An odd prime p is a sum of two squares (of integers) iff $p \equiv 1 \pmod 4$.*

Proof. As $x^2, y^2 \equiv 0$ or $1 \pmod 4$, so $x^2 + y^2 \equiv 0$ or 1 or $2 \pmod 4$. Assuming $p = x^2 + y^2$, then as p is odd, we have $p \equiv 1 \pmod 4$.

Conversely, assume $p \equiv 1 \pmod 4$, and, knowing that then $\left(\frac{-1}{p}\right) = 1$, take $r \in \mathbb{N}$ with $r^2 \equiv -1 \pmod p$. Define $f(u, v) = u + rv$ and $K = \lfloor \sqrt{p} \rfloor$. Note that

$$K < \sqrt{p} < K + 1, \tag{13}$$

as $\sqrt{p} \notin \mathbb{Z}$. Consider all pairs (u, v) with $0 \leq u \leq K$ and $0 \leq v \leq K$. There are $(K+1)^2 > p$ such pairs, and so the multiset of all $f(u, v)$ for such u, v has, by the Pigeonhole Principle, two such pairs $(u_1, v_1) \neq (u_2, v_2)$ for which $f(u_1, v_1) \equiv f(u_2, v_2) \pmod p$. Hence

$$\begin{aligned} u_1 + rv_1 &\equiv u_2 + rv_2 \pmod p \\ u_1 - u_2 &\equiv -r(v_1 - v_2) \pmod p \\ a &\equiv -rb \pmod p, \end{aligned}$$

say, where $a = u_1 - v_1$ and $b = v_1 - v_2$ are not both 0. Hence $a^2 \equiv -b^2 \pmod p$ as $r^2 \equiv -1 \pmod p$, so that $p \mid (a^2 + b^2)$. But $|a| \leq K$, $|b| \leq K$, giving

$$0 < a^2 + b^2 \leq 2K^2 < 2p.$$

So $a^2 + b^2 = p$. □

6.2. **The general case.** We now look at what happens if a prime $\equiv -1 \pmod 4$ *divides* a sum of two squares.

Proposition 6.2. *Let $q \equiv 3 \pmod 4$ be prime, and $q \mid (x^2 + y^2)$. Then $q \mid x$ and $q \mid y$, so that $q^2 \mid (x^2 + y^2)$.*

Proof. Assume that it is not the case that both x and y are divisible by q, say $q \nmid x$. Then from $x^2 + y^2 \equiv 0 \pmod q$ we get $(yx^{-1})^2 \equiv -1 \pmod q$, contradicting $\left(\frac{-1}{q}\right) = -1$. □

Proposition 6.3. *If n is a sum of two squares and m is a sum of two squares then so is nm.*

Proof. If $n = a^2 + b^2$ and $m = c^2 + d^2$ then

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

□

(This identity comes from complex numbers:

$$(a + ib)(c + id) = ac - bd + i(ad + bc)$$

gives

$$|a + ib|^2 \cdot |c + id|^2 = |ac - bd + i(ad + bc)|^2$$

and hence the identity.)

Corollary 6.4. *If $n = A^2 \prod_i n_i$ where $A, n_i \in \mathbb{Z}$ and each n_i is a sum of two squares, then so is n.*

Proof. Use induction on i to get $n/A^2 = \prod_i n_i = a^2 + b^2$ say. Then $n = (Aa)^2 + (Ab)^2$. □

We can now state and prove our main result.

Theorem 6.5 (Fermat)**.** *Write n in factorised form as*

$$n = 2^{f_2} \prod_{p \equiv 1 \pmod 4} p^{f_p} \prod_{q \equiv -1 \pmod 4} q^{g_q},$$

where (of course) all the p's and q's are prime. Then n can be written as the sum of two squares of integers iff all the g_q's are even.

Proof. If all the g_q are even then $n = A^2 \times$(product of some p's) and also $\times 2$ if f_2 is odd. So we have $n = A^2 \times \prod_i (a_i^2 + b_i^2)$ by Theorem 6.1 (using also $2 = 1^2 + 1^2$ if f_2 odd). Hence, by Corollary 6.4, n is the sum of two squares.

Conversely, suppose $q \mid n = a^2 + b^2$, where $q \equiv -1 \pmod 4$ is prime. Let q^k be the highest power of q dividing both a and b, so say $a = q^k a_1$, $b = q^k b_1$. Then

$$\frac{n}{q^{2k}} = a_1^2 + b_1^2.$$

Now $q \nmid \frac{n}{q^{2k}}$, as otherwise q would divide both a_1 and b_1, by Prop. 6.2. Hence q^{2k} is the highest power of q dividing n, i.e., $g_q = 2k$ is even. Hence all the g_q's are even. □

6.3. **Related results.**

Proposition 6.6. *If an integer n is the sum of two squares of rationals then it's the sum of two squares of integers.*

Proof. Suppose that

$$n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

for some rational numbers a/b and c/d. Then

$$n(bd)^2 = (da)^2 + (bc)^2.$$

Hence, by Thm 6.5, for every prime $q \equiv -1 \pmod 4$ with $q^i || n(bd)^2$, i must be even. But then if $q^\ell || bd$ then $q^{i-2\ell} || n$, with $i - 2\ell$ even. Hence, by Thm 6.5 (in the other direction), n is the sum of two squares of integers. □

Corollary 6.7. *A rational number n/m is the sum of two squares of rationals iff nm is the sum of two squares of integers.*

Proof. If $nm = a^2 + b^2$ for $a, b \in \mathbb{Z}$ then

$$\frac{n}{m} = \left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2.$$

Conversely, if

$$\frac{n}{m} = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

then

$$nm = \left(\frac{am}{b}\right)^2 + \left(\frac{cm}{d}\right)^2.$$

Hence, by Prop. 6.6, nm is the sum of two squares of integers. □

6.4. **Finding all ways of expressing a rational as a sum of two rational squares.** Now let h be a rational number that can be written as the sum of two squares of rationals. We can then describe *all* such ways of writing h.

Theorem 6.8. *Suppose that $h \in \mathbb{Q}$ is the sum of two rational squares: $h = s^2 + t^2$, where $s, t \in \mathbb{Q}$. Then the general solution of $h = x^2 + y^2$ in rationals x, y is*

$$x = \frac{s(u^2 - v^2) - 2uvt}{u^2 + v^2} \qquad y = -\left(\frac{t(u^2 - v^2) + 2uvs}{u^2 + v^2}\right), \tag{14}$$

where $u, v \in \mathbb{Z}$ not both zero.

Proof. We are looking for all points $(x, y) \in \mathbb{Q}^2$ on the circle $x^2 + y^2 = h$. If (x, y) is such a point, then for $x \neq s$ the chord through (s, t) and (x, y) has rational slope $(t - y)/(s - x)$.

Conversely, take a chord through (s, t) of rational slope r, which has equation $y = r(x - s) + t$. Then for the intersection point (x, y) of the chord and the circle we have

$$x^2 + (r(x - s) + t)^2 = h,$$

which simplifies to

$$x^2(1+r^2)+2rx(t-rs)+(r^2-1)s^2-2rst=0,$$

using the fact that $t^2-h=-s^2$. This factorises as

$$(x-s)((1+r^2)x+2rt+s(1-r^2))=0.$$

For $x\neq s$ we have

$$x=\frac{s(r^2-1)-2rt}{1+r^2}$$

and

$$\begin{aligned} y &= t+r(x-s) \\ &= -\left(\frac{t(r^2-1)+2sr}{1+r^2}\right), \end{aligned}$$

on simplification. Finally, substituting $r=u/v$ gives (14). Note that $v=0$ in (14) (i.e., $r=\infty$) gives the point $(r,-s)$. □

Corollary 6.9. *The general integer solution x,y,z of the equation $x^2+y^2=nz^2$ is*

$$(x,y,z)=(a(u^2-v^2)-2uvb, b(u^2-v^2)+2uva, u^2+v^2),$$

where $n=a^2+b^2$, with $a,b,u,v\in\mathbb{Z}$, and u,v arbitrary.

(If n is not the sum of two squares, then the equation has no nonzero solution, by Prop. 6.6.)

In particular, for $n=1=1^2+0^2$, we see that the general integer solution to Pythagoras' equation $x^2+y^2=z^2$ is

$$(x,y,z)=(u^2-v^2,2uv,u^2+v^2).$$

For a socalled *primitive* solution — one with $\gcd(x,y)=1$ – choose u,v with $\gcd(u,v)=1$ and not both odd.

The same method works for $Ax^2+By^2+Cz^2=0$.

6.5. **Sums of three squares, sums of four squares.**

Proposition 6.10. *No number of the form $4^a(8k+7)$, where a is a nonnegative integer, is the sum of three squares (of integers).*

Proof. Use induction on a. For $a=0$: Now $n^2\equiv 0,1$ or $4 \pmod 8$, so a sum of three squares is $\equiv 1$ or 1 or 2 or 3 or 4 or 5 or $6 \pmod 8$, but $\not\equiv 7 \pmod 8$.

Assume result true for some integer $a\geq 0$. If $4^{a+1}(8k+7)=n_1^2+n_2^2+n_3^2$ then all the n_i must be even, and so $=4(n_1'^2+n_2'^2+n_3'^2)$ say. But then $4^a(8k+7)=n_1'^2+n_2'^2+n_3'^2$, contrary to the induction hypothesis. □

In fact (won't prove)

Theorem 6.11 (Legendre 1798, Gauss)**.** *All positive integers except those of the form $4^a(8k+7)$ are the sum of three squares.*

Assuming this result, we can show

Corollary 6.12 (Lagrange 1770)**.** *Every positive integer is the sum of four squares.*

Proof. The only case we need to consider is $n = 4^a(8k+7)$. But then $n - (2^a)^2 = 4^a(8k+6) = 2^{2k+1}(4k+3)$, which (being exactly divisible by an odd power of 2) is not of the form $4^{a'}(8k'+7)$, so is the sum of three squares. □

7. Fermat's method of descent

Around 1640, Fermat developed a method for showing that an equation had no integer solutions. In essence, the method is as follows: assume that the equation *does* have a solution. Pick the 'smallest' (suitably defined) one. Use the assumed solution to construct a smaller solution, contradicting the fact that the one you started with was the smallest. This contradiction proves that there is in fact no solution. The technique is called *Fermat's method of descent.* It is, in fact, a form of strong induction. (Why?)

We illustrate the method with one example:

Theorem 7.1. *The equation*

$$x^4 + y^4 = z^2 \tag{15}$$

has no solution in positive integers x, y, z.

Corollary 7.2 (Fermat's Last Theorem for exponent 4)**.** *The equation $x^4 + y^4 = z^4$ has no solution in positive integers x, y, z.*

Proof of Theorem 7.1. (From H. Davenport, *The higher arithmetic. An introduction to the theory of numbers*, Longmans 1952, p.162). Suppose that (15) has such a solution. Assume we have a solution with $|z|$ minimal. We can clearly assume that z is positive and $\neq 1$, i.e., that $z > 1$. If $d = \gcd(x, y) > 1$ we can divide by d^4, replacing x by x/d, y by y/d and z by z/d^2 in (15), obtaining a solution with $|z|$ smaller. So we must have $\gcd(x, y) = 1$.

Now from Corollary 6.9 we know that

$$X^2 + Y^2 = Z^2$$

has general solution (with $\gcd(X, Y) = 1$), possibly after interchanging X and Y of

$$X = p^2 - q^2 \qquad Y = 2pq \qquad Z = p^2 + q^2,$$

where $p, q \in \mathbb{N}$ and $\gcd(p, q) = 1$, so

$$x^2 = p^2 - q^2 \qquad y^2 = 2pq \qquad z = p^2 + q^2.$$

As a square is $\equiv 0$ or $1 \pmod 4$, and x is odd (because $\gcd(x, y) = 1$), we see that p is odd and q is even, say $q = 2r$. So

$$x^2 = p^2 - (2r)^2 \qquad \left(\frac{y}{2}\right)^2 = pr.$$

Since $\gcd(p, r) = 1$ and pr is a square, we have $p = v^2$ and $r = w^2$ say, so

$$x^2 + (2w^2)^2 = v^4.$$

Note that, as $\gcd(p,q)=1$, we have $\gcd(x,q)=1=\gcd(x,2w^2)$. Hence applying Corollary 6.9 again

$$x=p_1^2-q_1^2 \qquad 2w^2=2p_1q_1 \qquad v^2=p_1^2+q_1^2,$$

where $\gcd(p_1,q_1)=1$ and not both are odd. Say p_1 odd, q_1 even. Thus $w^2=p_1q_1$, giving $p_1=v_1^2$, $q_1=r_1^2$, say. Hence

$$v^2(=p_1^2+q_1^2)=v_1^4+r_1^4,$$

which is another solution of (15)! But

$$v^2=p=\sqrt{z-q^2}<\sqrt{z},$$

giving $v<z^{1/4}$, so certainly $v<z$ (as $z>1$), contradicting the minimality of z. □

8. p-ADIC NUMBERS

8.1. **Motivation: Solving $x^2\equiv a \pmod{p^n}$.** Take an odd prime p, and an integer a coprime to p. Then, as we know, $x^2\equiv a \pmod p$ has a solution $x\in\mathbb{Z}$ iff $\left(\frac{a}{p}\right)=1$. In this case we can suppose that $b_0^2\equiv a \pmod p$. We claim that then $x^2\equiv a \pmod{p^n}$ has a solution x for all $n\in\mathbb{N}$.

Assume that we have a solution x of $x^2\equiv a \pmod{p^n}$ for some $n\geq 1$. Then x is coprime to p, so that we can find $x_1\equiv \frac{1}{2}(x+a/x) \pmod{p^{2n}}$. (This is the standard Newton-Raphson iterative method $x_1=x-f(x)/f'(x)$ for solving $f(x)=0$, applied to the polynomial $f(x)=x^2-a$, but $\pmod{p^{2n}}$ instead of in $\mathbb{R}$ or $\mathbb{C}$.) Then

$$x_1-x=-\frac{1}{2}\left(x-\frac{a}{x}\right)=-\frac{1}{2x}\left(x^2-a\right)\equiv 0 \pmod{p^n},$$

and

$$\begin{aligned} x_1^2-a &= \frac{1}{4}\left(x^2+2a+\frac{a^2}{x^2}\right)-a \\ &= \frac{1}{4}\left(x-\frac{a}{x}\right)^2 \\ &= \frac{1}{4x^2}(x^2-a)^2 \\ &\equiv 0 \pmod{p^{2n}} \end{aligned}$$

Thus, starting with x_0 such that $x_0^2\equiv a \pmod{p^{2^0}}$, we get successively x_1 with $x_1^2\equiv a \pmod{p^{2^1}}$, x_2 with $x_2^2\equiv a \pmod{p^{2^2}}$,..., x_k with $x_k^2\equiv a \pmod{p^{2^k}}$,..., with $x_{k+1}\equiv x_k \pmod{p^{2^k}}$. So, writing the x_i in base p, we obtain

$$\begin{aligned} &x_0=b_0 \\ &x_1=b_0+b_1p && \text{say, specified} && \pmod{p^2} \\ &x_2=b_0+b_1p+b_2p^2+b_3p^3 && \text{say, specified} && \pmod{p^4} \\ &x_3=b_0+b_1p+b_2p^2+b_3p^3+b_4p^4+b_5p^5+b_6p^6+b_7p^7 && \text{say, specified} && \pmod{p^8}, \end{aligned}$$

and so on.

So, in any sense, is $x_\infty = \sum_{i=1}^{\infty} b_i p^i$ a root of $x^2 \equiv a \pmod{p^\infty}$? It turns out that, yes, it is: x_∞ is a root of $x^2 = a$ in the field $\mathbb{Q}_p$ of p-adic numbers.

8.2. **Valuations.** In order to define the fields $\mathbb{Q}_p$ of p-adic numbers for primes p, we first need to discuss valuations.

A *valuation* $|\cdot|$ on a field F is a map from F to the nonnegative real numbers satisfying

$$\text{For each } x \in F \qquad |x| = 0 \text{ iff } x = 0; \qquad \text{(ZERo)}$$

$$\text{For each } x, y \in F \qquad |xy| = |x| \cdot |y|; \qquad \text{(HOMomorphism)}$$

$$\text{For each } x, y \in F \qquad |x + y| \le |x| + |y|. \qquad \text{(TRIangle)}$$

If in addition

$$\text{For each } x, y \in F \qquad |x + y| \le \max(|x|, |y|), \qquad \text{(MAXimum)}$$

then $|\cdot|$ is called a *nonarchimedean* valuation. A valuation that is not nonarchimedean, i.e., for which there exist $x, y \in F$ such that $|x + y| > \max(|x|, |y|)$, is called *archimedean*. For instance the standard absolute value on $\mathbb{R}$ is archimedean because $2 = |2| = |1 + 1| > \max(|1|, |1|) = 1$.

Note that MAX is stronger than TRI in the sense that if MAX is true than TRI is certainly true. So to show that a valuation is nonarchimedean we only need to check that ZER, HOM and MAX hold.

Proposition 8.1. *For any valuation $|\cdot|$ on a field F we have $|1| = |-1| = 1$ and for $n \in \mathbb{N}$ (defined as the sum of n copies of the identity of F) we have $|-n| = |n|$ and $|1/n| = 1/|n|$. Further, for $n, m \in N$ we have $|n/m| = |n|/|m|$.*

Proof. We have $|1| = |1^2| = |1|^2$, using HOM, so that $|1| = 0$ or 1. But $|1| \neq 0$ by ZER, so $|1| = 1$.

Also $1 = |1| = |(-1)^2| = |-1|^2$ by HOM, so that $|-1| = 1$ since $|-1| > 0$.

Further, $|-n| = |(-1)n| = |-1| \cdot |n| = 1 \cdot |n| = |n|$, and from $n \cdot (1/n) = 1$ we get $|n| \cdot |1/n| = |1| = 1$, so that $|1/n| = 1/|n|$.

Finally, from $n/m = n \cdot (1/m)$ we get $|n/m| = |n| \cdot |1/m| = |n|/|m|$. □

8.3. **Nonarchimedean valuations.** From now on we restrict our attention to nonarchimedean valuations.

Proposition 8.2 (Principle of Domination)**.** *Suppose that we have a nonarchimedean valuation $|\cdot|$ on a field F, and that $x, y \in F$ with $|x| \neq |y|$. Then*

$$|x + y| = \max(|x|, |y|).$$

Note the equal sign in this statement!

Proof. Put $s = x + y$, and assume w.l.g. that $|x| < |y|$. Then $|s| \le \max(|x|, |y|) = |y|$, while

$$|y| = |s - x| \le \max(|s|, |-x|) = \max(|s|, |x|) = |s|,$$

since otherwise we'd have $|y| \le |x|$. Hence $|s| = |y| = \max(|x|, |y|)$. □

Corollary 8.3. *Suppose that $x_1, \ldots, x_n \in F$, with $|\cdot|$ nonarchimedean. Then*

$$|x_1 + \ldots, +x_n| \leq \max(|x_1|, \ldots, |x_n|),$$

with equality if $|x_1| > \max(|x_2, \ldots, |x_n|)$.

Proof. Use induction, with the help of MAX, for the inequality. For the equality, put $x_1 = y$ and $x_2 + \cdots + x_n = x$ in the Principle of Domination. □

Corollary 8.4. *For $|\cdot|$ nonarchimedean and $n \in \mathbb{Z}$ we have $|n| \leq 1$.*

Proof. Apply the Corollary above with all $x_i = 1$. Then use $|-n| = |n|$. □

Lemma 8.5. *If $|\cdot|$ is a nonarchimedean valuation on F, then so is $|\cdot|^\alpha$ for any $\alpha > 0$.*

Proof. It's easily checked that ZER, HOM and MAX still hold when the valuation we start with is taken to the α-th power. □

[The same does *not* apply to TRI – we need $0 < \alpha \leq 1$ for TRI to still always hold.]

8.4. **Nonarchimedean valuations on $\mathbb{Q}$.**

Corollary 8.6. *If $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$ with $|n| = 1$ for all $n \in \mathbb{N}$ then $|\cdot|$ is trivial, i.e., $|x| = 0$ if $x = 0$ while $|x| = 1$ if $x \neq 0$.*

Proof. We then have $|x| = 0$ by ZER, while $|n/m| = |n|/|m| = 1/1 = 1$. □

We'll ignore trivial valuations from now on.

Proposition 8.7. *If $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$ with $|n| < 1$ for some $n \in \mathbb{N}$, then there is a prime p such that $\{n \in \mathbb{N} : |n| < 1\} = \{n \in \mathbb{N} : p \text{ divides } n\}$.*

Proof. Take the smallest positive integer n_1 such that $|n_1| < 1$. We know that $n_1 > 1$. If n_1 is composite, say $n_1 = n_2 n_3$ with $1 < n_2, n_3 < n_1$, then, by the minimality of n_1, we have $|n_2| = |n_3| = 1$, so that $|n_1| = |n_2| \cdot |n_3| = 1 \cdot 1 = 1$ by HOM, a contradiction. Hence n_1 is prime, $= p$ say.

Then for any n with $|n| < 1$ we can, by the division algorithm, write $n = qp + r$ where $0 \leq r < p$. But then $|r| = |n - qp| \leq \max(|n|, |-qp|) = \max(|n|, |-1| \cdot |q| \cdot |p|) < 1$, as $|-1| = 1$, $|q| \leq 1$ and $|p| < 1$. By the minimality of p we must have $r = 0$, so that $p \mid n$. □

Next, we show that there is indeed a valuation on $\mathbb{Q}$ corresponding to each prime p. We define $|\cdot|_p$ by $|0| = 0$, $|p|_p = 1/p$ and $|n| = 1$ for $n \in \mathbb{Z}$ and coprime to p, and $|p^k n/m|_p = p^{-k}$ for n and m coprime to p. We call this the *p-adic valuation* on $\mathbb{Q}$.

Proposition 8.8. *The p-adic valuation on $\mathbb{Q}$ is indeed a valuation.*

Proof. The definition of $|\cdot|_p$ ensures that ZER and HOM hold. It remains only to check that MAX holds.

Let $x = p^k n/m$ and $y = p^{k'} n'/m'$,where $n, m, n'm'$ are all coprime to p. Suppose w.l.g. that $k \leq k'$. Then $|x|_p = |p^k|_p \cdot |n|_p/|m|_p = p^{-k}$ as $|n|_p = |m|_p = 1$ and $|p|_p = 1/p$. Similarly $|y|_p = p^{-k'} \leq |x|_p$. Hence

$$|x+y|_p = \left|\frac{p^k(nm' + p^{k'-k}n'm)}{mm'}\right|_p = \frac{p^{-k}|nm' + p^{k'-k}n'm|_p}{|mm'|_p} \leq p^{-k} = \max(|x|_p, |y|_p).$$

as $|m|_p = |m'|_p = 1$ and $|nm' + p^{k'-k}n'm|_p \leq 1$, since $nm' + p^{k'-k}n'm \in \mathbb{Z}$. □

[Note that the choice of $|p|_p = 1/p$ is not particularly important, as by replacing $|\cdot|_p$ by its α-th power as in Lemma 8.5 we can make $|p|_p$ equal any number we like in the interval $(0, 1)$. But we do need to fix on a definite value!]

8.5. **The p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$.** We first recall how to construct the real field $\mathbb{R}$ from $\mathbb{Q}$, using Cauchy sequences. Take the ordinary absolute value $|\cdot|$ on $\mathbb{Q}$, and define a *Cauchy sequence* to be a sequence $(a_n) = a_1, a_2, \ldots, a_n, \ldots$ of rational numbers with the property that for each $\varepsilon > 0$ there is an $N > 0$ such that $|a_n - a_{n'}| < \varepsilon$ for all $n, n' > N$. We define an equivalence relation on these Cauchy sequences by saying that two such sequences (a_n) and (b_n) are *equivalent* if the interlaced sequence $a_1, b_1, a_2, b_2, \ldots, a_n, b_n, \ldots$ is also a Cauchy sequence. [Essentially, this means that the sequences tend to the same limit, but as we haven't yet constructed $\mathbb{R}$, where (in general) the limit lies, we can't say that.] Having checked that this is indeed an equivalence relation on these Cauchy sequences, we define $\mathbb{R}$ to be the set of all equivalence classes of such Cauchy sequences. We represent each equivalence class by a convenient equivalence class representative; one way to do this is by the standard decimal expansion. So, the class π will be represented by the Cauchy sequence $3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \ldots$, which we write as $3.14159\ldots$. Further, we can make $\mathbb{R}$ into a field by defining the sum and product of two Cauchy sequences in the obvious way, and also the reciprocal of a sequence, provided the sequence doesn't tend to 0.

[The general unique decimal representation of a real number a is

$$a = \pm 10^k(d_0 + d_1 10^{-1} + d_2 10^{-2} + \cdots + d_n 10^{-n} + \ldots),$$

where $k \in \mathbb{Z}$, and the digits d_i are in $\{0, 1, 2, \ldots, 9\}$, with $d_0 \neq 0$. Also, it is forbidden that the d_i's are all $= 9$ from some point on, as otherwise we get non-unique representations, e.g., $1 = 10^0(1.00000\ldots) = 10^{-1}(9.99999\ldots)$.]

We do the same kind of construction to define the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$, except that we replace the ordinary absolute value by $|\cdot|_p$ in the method to obtain *p-Cauchy sequences*. To see what we should take as the equivalence class representatives, we need the following result.

Lemma 8.9. *Any rational number m/n with $|m/n|_p = 1$ can be p-adically approximated arbitrarily closely by a positive integer. That is, for any $k \in \mathbb{N}$ there is an $N \in \mathbb{N}$ such that $|m/n - N|_p \leq p^{-k}$.*

Proof. We can assume that $|n|_p = 1$ and $|m|_p \leq 1$. We simply take $N = mn'$, where $nn' \equiv 1 \pmod{p^k}$. Then the numerator of $m/n - N$ is an integer that is divisible by p^k. □

An immediate consequence of this result is that *any* rational number (i.e., dropping the $|m/n|_p = 1$ condition) can be approximated arbitrarily closely by a positive integer times a power of p. Thus one can show that any p-Cauchy sequence is equivalent to one containing only those kind of numbers. We write the positive integer N in base p, so that $p^k N = p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r)$ say, where the a_i are base-p digits $\in \{0, 1, 2, \ldots, p-1\}$, and where we can clearly assume that $a_0 \neq 0$ (as otherwise we could increase k by 1). We define $\mathbb{Q}_p$, the *p-adic numbers*, to be the set of all equivalence classes of p-Cauchy sequences of elements of $\mathbb{Q}$. Then we have the following.

Theorem 8.10. *Every nonzero element (i.e., equivalence class) in $\mathbb{Q}_p$ has an equivalence class representative of the form*

$$p^k a_0, p^k(a_0 + a_1 p), p^k(a_0 + a_1 p + a_2 p^2), \ldots, p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_i p^i), \ldots,$$

which we write simply as

$$p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_i p^i + \ldots) \qquad [= p^k(\sum_{i=0}^{\infty} a_i p^i)].$$

Here, the a_i are all in $\in \{0, 1, 2, \ldots, p-1\}$, with $a_0 \neq 0$.

Thus we can regard p-adic numbers as these infinite sums $p^k(\sum_{i=0}^{\infty} a_i p^i)$. We define the unary operations of negation and reciprocal, and the binary operations of addition and multiplication in the natural way, namely: apply the operation to the (rational) elements of the p-Cauchy sequence representing that number, and then choose a standard equivalence class representative (i.e., $p^k(\sum_{i=0}^{\infty} a_i p^i)$ with all $a_i \in \{0, 1, 2, \ldots, p-1\}$, $a_0 \neq 0$) for the result. When we do this, we have

Theorem 8.11. *With these operations, $\mathbb{Q}_p$ is a field, the field of p-adic numbers, and the p-adic valuation $|\cdot|_p$ can be extended from $\mathbb{Q}$ to $\mathbb{Q}_p$ by defining $|a|_p = p^{-k}$ when $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$. Again, the a_i are all in $\in \{0, 1, 2, \ldots, p-1\}$, with $a_0 \neq 0$.*

We shall skip over the tedious details that need to be checked to prove these two theorems.

Note that, like $\mathbb{R}$, $\mathbb{Q}_p$ is an uncountable field of characteristic 0 (quite unlike $\mathbb{F}_p$, which is a finite field of characteristic p).

We define a *p-adic integer* to be an p-adic number a with $|a|_p \leq 1$, and $\mathbb{Z}_p$ to be the set of all p-adic integers.

Proposition 8.12. *With the arithmetic operations inherited from $\mathbb{Q}_p$, the set $\mathbb{Z}_p$ is a ring.*

Proof. This is simply because if a and $a' \in \mathbb{Z}_p$, then $|a|_p \leq 1$ and $|a'|_p \leq 1$, so that

$$\begin{aligned} |a + a'|_p &\leq \max(|a|_p, |a'|_p) && \leq 1 && \text{by MAX ;} \\ |a \cdot a'|_p &= |a|_p \cdot |a'|_p && \leq 1 && \text{by HOM ,} \end{aligned}$$

showing that $\mathbb{Z}_p$ is closed under both addition and multiplication, and so is a ring. $\square$

An p-adic number a is called a *p-adic unit* if $|a|_p = 1$. Then $k = 0$ so that $a = \sum_{i=0}^{\infty} a_i p^i$ with all $a_i \in \{0, 1, 2, \ldots, p-1\}$ and $a_0 \neq 0$. The set of all p-adic units is a multiplicative subgroup of the multiplicative group $\mathbb{Q}_p^\times = \mathbb{Q}_p \setminus \{0\}$. This is because if $|a|_p = 1$ then $|1/a|_p = 1/|a|_p = 1$, so that $1/a$ is also a unit.

8.6. **Calculating in $\mathbb{Q}_p$.**

8.6.1. *Negation.* If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, then

$$-a = p^k \left((p - a_0) + \sum_{i=1}^{\infty} (p - 1 - a_i) p^i \right),$$

as can be checked by adding a to $-a$ (and getting 0!). Note that from all $a_i \in \{0, 1, 2, \ldots, p-1\}$ and $a_0 \neq 0$ we have that the same applies to the digits of $-a$.

8.6.2. *Reciprocals.* If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, then

$$\frac{1}{a} = p^{-k}(a'_0 + a'_1 p + \cdots + a'_i p^i + \ldots)$$

say, where for any i the first i digits $a'_0, a'_1, \ldots, a'_i$ can be calculated as follows: Putting $a_0 + a_1 p + \cdots + a_i p^i = N$, calculate $N' \in \mathbb{N}$ with $N' < p^{i+1}$ such that $NN' \equiv 1 \pmod{p^{i+1}}$. Then writing N' in base p as $N' = a'_0 + a'_1 p + \cdots + a'_i p^i$ gives $a'_0, a'_1, \ldots, a'_i$.

8.6.3. *Addition and multiplication.* If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ and $a' = p^k(\sum_{i=0}^{\infty} a'_i p^i)$ (same k) then $a + a' = p^k((a_0 + a'_0) + (a_1 + a'_1)p + \cdots + (a_i + a'_i)p^i + \ldots)$, where then 'carrying' needs to be performed to get the digits of $a + a'$ into $\{0, 1, 2, \ldots, p-1\}$. If $a' = p^{k'}(\sum_{i=0}^{\infty} a'_i p^i)$ with $k' < k$ then we can pad the expansion of a' with initial zeros so that we can again assume that $k' = k$, at the expense of no longer having a'_0 nonzero. Then addition can be done as above.

Multiplication is similar: multiplying $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ by $a' = p^{k'}(\sum_{i=0}^{\infty} a'_i p^i)$ gives

$$a \cdot a' = p^{k+k'}(a_0 a'_0 + (a_1 a'_0 + a_0 a'_1)p + \cdots + (\sum_{j=0}^{i} a_j a'_{i-j})p^i + \ldots),$$

where then this expression can be put into standard form by carrying.

8.7. **Expressing rationals as p-adic numbers.** Any nonzero rational can clearly be written as $\pm p^k m/n$, where m, n are positive integers coprime to p (and to each other), and $k \in \mathbb{Z}$. It's clearly enough to express $\pm m/n$ as a p-adic number $a_0 + a_1 p + \ldots$, as then $\pm p^k m/n = p^k(a_0 + a_1 p + \ldots)$.

8.7.1. *Representating $-m/n$, where $0 < m < n$.* We have the following result.

Proposition 8.13. *Put $e = \varphi(n)$. Suppose that m and n are coprime to p, with $0 < m < n$, and that the integer*

$$m\frac{p^e - 1}{n} \qquad \textit{is written as} \qquad d_0 + d_1 p + \cdots + d_{e-1}p^{e-1}$$

in base p. Then

$$-\frac{m}{n} = d_0 + d_1 p + \cdots + d_{e-1}p^{e-1} + d_0 p^e + d_1 p^{e+1} + \cdots + d_{e-1}p^{2e-1} + d_0 p^{2e} + d_1 p^{2e+1} + \dots.$$

Proof. We know that $\frac{p^e-1}{n}$ is an integer, by Euler's Theorem. Hence

$$-\frac{m}{n} = \frac{m\frac{p^e-1}{n}}{1-p^e} = (d_0 + d_1 p + \cdots + d_{e-1}p^{e-1})(1 + p^e + p^{2e} + \dots),$$

which gives the result. □

In the above proof, we needed $m < n$ so that $m\frac{p^e-1}{n} < p^e$, and so had a representation $d_0 + d_1 p + \cdots + d_{e-1}p^{e-1}$.

8.7.2. *The case m/n, where $0 < m < n$.* For this case, first write $-m/n = u/(1-p^e)$, where, as above, $u = m \cdot \frac{p^e-1}{n}$. Then

$$\frac{m}{n} = \frac{-u}{1-p^e} = 1 + \frac{p^e - 1 - u}{1-p^e} = 1 + \frac{u'}{1-p^e},$$

where $u' = p^e - 1 - u$ and $0 \le u' < p^e$. Thus we just have to add 1 to the repeating p-adic integer $u' + u'p^e + u'p^{2e} + \dots$.

Example What is $1/7$ in $\mathbb{Q}_5$?
From $5^6 \equiv 1 \pmod 7$ (Fermat), and $(5^6 - 1)/7 = 2232$, we have

$$\begin{aligned} -\frac{1}{7} &= \frac{2232}{1-5^6} \\ &= \frac{2 + 1\cdot 5 + 4\cdot 5^2 + 2\cdot 5^3 + 3\cdot 5^4}{1-5^6} \\ &= (21423)(1 + 5^6 + 5^{12} + \dots) \\ &= 214230\,214230\,214230\,214230\,214230\dots. \end{aligned}$$

Hence

$$\frac{1}{7} = 330214\,230214\,230214\,230214\,230214\,230214\dots,$$

which is a way of writing $3 + 3\cdot 5^1 + 0\cdot 5^2 + 2\cdot 5^3 + \dots$.

8.8. **Taking square roots in $\mathbb{Q}_p$.**

8.8.1. *The case of p odd.* First consider a p-adic unit $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$, where p is odd. Which such a have a square root in $\mathbb{Q}_p$? Well, if $a = b^2$, where $b = b_0 + b_1 p + b_2 p^2 + \cdots \in \mathbb{Z}_p$, then, working modulo p we see that $a_0 \equiv b_0^2 \pmod{p}$, so that a_0 must be a quadratic residue $\pmod{p}$. In this case the method in Section 8.1 will construct b. Note that if at any stage you are trying to construct $b \pmod{n}$ then you only need to specify $a \pmod{n}$, so that you can always work with rational integers rather than with p-adic integers.

On the other hand, if a_0 is a quadratic nonresidue, then a has no square root in $\mathbb{Q}_p$.

Example. Computing $\sqrt{6}$ in $\mathbb{Q}_5$. While the algorithm given in the introduction to this chapter is a good way to compute square roots by computer, it is not easy to use by hand. Here is a simple way to compute square roots digit-by-digit, by hand: Write $\sqrt{6} = b_0 + b_1 \cdot 5^1 + b_2 \cdot 5^2 + \ldots$. Then, squaring and working mod 5, we have $b_0^2 \equiv 1 \pmod{5}$, so that $b_0 = 1$ or 4. Take $b_0 = 1$ (4 will give the other square root, which is minus the one we're computing.)

Next, working mod 5^2, we have

$$\begin{aligned} 6 &\equiv (1 + b_1 \cdot 5)^2 \pmod{5^2} \\ 6 &\equiv 1 + 10 b_1 \pmod{5^2} \\ 1 &\equiv 2 b_1 \pmod{5}, \end{aligned}$$

giving $b_1 = 3$. Doing the same thing mod 5^3 we have

$$\begin{aligned} 6 &\equiv (1 + 3 \cdot 5 + b_2 \cdot 5^2)^2 \pmod{5^3} \\ 6 &\equiv 16^2 + 32 b_2 \cdot 5^2 \pmod{5^3} \\ -250 &\equiv 32 b_2 \cdot 5^2 \pmod{5^3} \\ 0 &\equiv 32 b_2 \pmod{5}, \end{aligned}$$

giving $b_2 = 0$. Continuing mod 5^4, we get $b_3 = 4$, so that $\sqrt{6} = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \ldots$.

Next, consider a general p-adic number $a = p^k(a_0 + a_1 p + \ldots)$. If $a = b^2$, then $|a|_p = |b|_p^2$, so that $|b|_p = |a|_p^{1/2} = p^{-k/2}$. But valuations of elements of $\mathbb{Q}_p$ are integer powers of p, so that if k is odd then $b \notin \mathbb{Q}_p$. But if k is even, there is no problem, and a will have a square root $b = p^{k/2}(b_0 + b_1 p + \ldots) \in \mathbb{Q}_p$ iff a_0 is a quadratic residue $\pmod{p}$.

8.8.2. *The case of p even.* Consider a 2-adic unit $a = 1 + a_1 2 + a_2 2^2 + \cdots \in \mathbb{Z}_2$. If $a = b^2$, where $b = b_0 + b_1 2^1 + b_2 2^2 + \cdots \in \mathbb{Z}_2$, working modulo 8, we have $b^2 \equiv 1 \pmod{8}$, so that we must have $a \equiv 1 \pmod{8}$, giving $a_1 = a_2 = 0$. When this holds, the construction of Section 8.1 will again construct b. On the other hand, if $a \not\equiv 1 \pmod{8}$, then a has no square root in $\mathbb{Q}_2$.

For a general 2-adic number $a = 2^k(1 + a_1 2 + a_2 2^2 + \ldots)$, we see that, similarly to the case of p odd, a will have a square root in $\mathbb{Q}_2$ iff k is even and $a_1 = a_2 = 0$.

8.9. **The Local-Global Principle.** The fields $\mathbb{Q}_p$ (p prime) and $\mathbb{R}$, and their finite extensions, are examples of *local fields*. These are *complete* fields, because they contain all their limit points. On the other hand, $\mathbb{Q}$ and its finite extensions are called *number fields* and are examples of *global fields*. [Other examples of global and local fields are the fields $\mathbb{F}(x)$ of rational functions over a finite field $\mathbb{F}$ (global) and their completions with respect to the valuations on them (local).] One associates to a global field the local fields obtained by taking the completions of the field with respect to each valuation on that field.

Suppose that you are interested in whether an equation $f(x, y) = 0$ has a solution x, y in rational numbers. Clearly, if the equation has no solution in $\mathbb{R}$, or in some $\mathbb{Q}_p$, then, since these fields contain $\mathbb{Q}$, the equation has no solution on $\mathbb{Q}$ either.

For example, the equation $x^2 + y^2 = -1$ has no solution in $\mathbb{Q}$ because it has no solution in $\mathbb{R}$. The equation $x^2 + 3y^2 = 2$ has no solution in $\mathbb{Q}$ because it has no solution in $\mathbb{Q}_3$, because 2 is a quadratic nonresidue of 3.

The Local-Global (or Hasse-Minkowski) Principle is said to hold for a class of equations (over $\mathbb{Q}$, say) if, whenever an equation in that class has a solution in each of its completions, it has a solution in $\mathbb{Q}$. This principle holds, in particular, for quadratic forms. Thus for such forms in three variables, we have the following result.

Theorem 8.14. *Let a, b, c be nonzero integers, squarefree, pairwise coprime and not all of the same sign. Then the equation*

$$ax^2 + by^2 + cz^2 = 0 \tag{16}$$

has a nonzero solution $(x, y, z) \in \mathbb{Z}^3$ iff
$-bc$ is a quadratic residue of a; i.e. the equation $x^2 \equiv -bc \pmod{a}$ has a solution x;
$-ca$ is a quadratic residue of b;
$-ab$ is a quadratic residue of c.

(Won't prove.) The first of these conditions is necessary and sufficient for (16) to have a solution in $\mathbb{Q}_p$ for each odd prime dividing a. Similarly for the other two conditions. The condition that a, b, c are not all of the same sign is clearly necessary and sufficent that (16) has a solution in $\mathbb{R}$. But what about a condition for a solution in $\mathbb{Q}_2$?

8.9.1. *Hilbert symbols.* It turns out that we don't need to consider solutions in $\mathbb{Q}_2$, because if a quadratic form has no solution in $\mathbb{Q}$ then it has no solution in a positive, even number (so, at least 2!) of its completions. Hence, if we've checked that it has a solution in all its completions except one, it must in fact have a solution in all its completions, and so have a solution in $\mathbb{Q}$. This is best illustrated by using Hilbert symbols and Hilbert's Reciprocity Law.

For $a, b \in \mathbb{Q}$ the Hilbert symbol $(a, b)_p$, where p is a prime or ∞, and $\mathbb{Q}_\infty = \mathbb{R}$, is defined by

$$(a, b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a nonzero solution in } \mathbb{Q}_p; \\ -1 & \text{otherwise.} \end{cases}$$

Hilbert's Reciprocity Law says that $\prod_p (a,b)_p = 1$. (Won't prove; it is, however, essentially equivalent to the Law of Quadratic Reciprocity.) Hence, a finite, even number of $(a,b)_p$ (p a prime or ∞) are equal to -1.

8.10. **Nonisomorphism of $\mathbb{Q}_p$ and $\mathbb{Q}_q$.** When one writes rational numbers to any (integer) base $b \geq 2$, and then forms the completion with respect to the usual absolute value $|\cdot|$, one obtains the real numbers $\mathbb{R}$, (though maybe written in base b). Thus the field obtained ($\mathbb{R}$) is independent of b. Furthermore, b needn't be prime.

However, when completing $\mathbb{Q}$ (in whatever base) with respect to the p-adic valuation to obtain $\mathbb{Q}_p$, the field obtained *does* depend on p, as one might expect, since a different valuation is being used for each p. One can, however, prove this directly:

Theorem 8.15. *Take p and q to be two distinct primes. Then $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic.*

Proof. We can assume that p is odd. Suppose first that q is also odd. Let n be a quadratic nonresidue $\pmod q$. Then using the Chinese Remainder Theorem we can find $k, \ell \in \mathbb{N}$ with $1+kp = n+\ell q$. Hence, for $a = 1+kp$ we have $\left(\frac{a}{p}\right) = \left(\frac{1}{p}\right) = 1$ while $\left(\frac{a}{q}\right) = \left(\frac{n}{q}\right) = -1$. Hence, by the results of Subsection 8.8 we see that $\sqrt{a} \in \mathbb{Q}_p$ but $\sqrt{a} \notin \mathbb{Q}_q$. Thus, if there were an isomorphism $\phi : \mathbb{Q}_p \to \mathbb{Q}_q$ then we'd have

$$\phi(\sqrt{a})^2 = \phi(\sqrt{a}^2) = \phi(a) = \phi(1+1+\cdots+1) = a,$$

so that $\phi(\sqrt{a})$ *would* be a square root of a in $\mathbb{Q}_q$, a contradiction.

Similarly, if $q = 2$ then we can find $a = 1 + kp = 3 + 4\ell$, so that $\sqrt{a} \in \mathbb{Q}_p$ again, but $\sqrt{a} \notin \mathbb{Q}_2$. so the same argument applies. □

Note that for any integer $b \geq 2$ one can, in fact, define the ring of b-adic numbers, which consists of numbers $p^k(a_0 + a_1 b + a_2 b^2 + \cdots + a_i b^i + \dots)$, where $k \in \mathbb{Z}$ and all $a_i \in \{0, 1, 2, \dots, b-1\}$. However, if b is composite, this ring has nonzero zero divisors (nonzero numbers a, a' such that $aa' = 0$), so is not a field. See problem sheet 5 for the example $b = 6$.

9. Some Analytic Results about primes and the divisor function

9.1. **The Prime Number Theorem.** How frequent are the primes? At the end of the eighteenth century, Gauss and Legendre suggested giving up looking for a formula for the nth prime, and proposed instead estimating the number of primes up to x. So, define the prime-counting function $\pi(x)$ by

$$\pi(x) = \sum_{\substack{p \leq x \\ p \text{ prime}}} 1.$$

Gauss conjectured on computational evidence that $\pi(x) \sim \frac{x}{\log x}$. This was proved by independently by Hadamard and de la Vallée Poussin in 1896, and became known as

Theorem 9.1 (The Prime Number Theorem)**.** *We have $\pi(x) \sim \frac{x}{\log x}$ as $x \to \infty$.*

It turns out to be more convenient to work with

$$\theta(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} \log p,$$

which is called *Chebyshev's θ-function*. In terms of this function it can be shown (not difficult) that the Prime Number Theorem is equivalent to the statement $\theta(x) \sim x \quad (x \to \infty)$.

We won't prove PNT here, but instead a weaker version, and in terms of $\theta(x)$:

Theorem 9.2. *As $x \to \infty$ we have*

$$(\log 2)x + o(x) < \theta(x) < (2\log 2)x + o(x),$$

so that

$$0.6931x + o(x) < \theta(x) < 1.3863x + o(x).$$

9.2. **Proof of Theorem 9.2.**

9.2.1. *The upper bound.*

Proposition 9.3. *We have $\theta(x) < (2\log 2)x + O(\log^2 x)$.*

Proof. Consider $\binom{2n}{n}$. By the Binomial Theorem, it is less than $(1+1)^{2n} = 4^n$. Also, it is divisible by all primes p with $n < p \le 2n$, so

$$4^n > \binom{2n}{n} \ge \prod_{n<p\le 2n} p = e^{\theta(2n)-\theta(n)}.$$

Hence $\theta(2n) - \theta(n) \le 2n\log 2$.

Now if $2n \le x < 2n+2$ (i.e., $n \le x/2 < n+1$) then $\theta(x/2) = \theta(n)$ and

$$\theta(x) \le \theta(2n) + \log(2n+1) \le \theta(2n) + \log(x+1),$$

so that, for each x,

$$\begin{aligned}\theta(x) - \theta(x/2) &\le \theta(2n) + \log(x+1) - \theta(n)\\ &\le 2n\log 2 + \log(x+1)\\ &\le x\log 2 + \log(x+1).\end{aligned}$$

So (standard telescoping argument for $x, x/2, x/2^2, \ldots, x/2^k$ where $x/2^{k-1} \ge 2$, $x/2^k < 2$, $\theta(x/2^k) = 0$):

$$\begin{aligned}\theta(x) &= \left(\theta(x) - \theta\left(\frac{x}{2}\right)\right) + \left(\theta\left(\frac{x}{2}\right) - \theta\left(\frac{x}{2^2}\right)\right) + \left(\theta\left(\frac{x}{2^2}\right) - \theta\left(\frac{x}{2^3}\right)\right) + \ldots \left(\theta\left(\frac{x}{2^{k-1}}\right) - \theta\left(\frac{x}{2^k}\right)\right)\\ &\le \log 2\left(x + \frac{x}{2} + \cdots + \frac{x}{2^{k-1}}\right) + k\log(x+1)\\ &\le 2x\log 2 + \lfloor \log_2 x \rfloor \log(x+1)\\ &\le 2x\log 2 + O(\log^2 x).\end{aligned}$$

□

9.2.2. *The lower bound.* To obtain an inequality in the other direction, we look at

$$d_n = \operatorname{lcm}(1, 2, \dots, n) = e^{\sum_{p^m \le n} \log p}.$$

Define

$$\psi(x) = \sum_{\substack{p^m \le x \\ p \text{ prime}}} \log p;$$

(i.e., $\log p$ to be counted m times if p^m is the highest power of p that is $\le x$). So $d_n = e^{\psi(n)}$.

Lemma 9.4. *We have* $\psi(x) < \theta(x) + 2x^{1/2} \log x + O(\log^2 x)$.

Proof. Now

$$\begin{aligned}\psi(x) &= \sum_{p \le x} \log x + \sum_{p^2 \le x} \log x + \sum_{p^3 \le x} \log x + \dots \\ &= \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \dots + \theta(x^{1/k}),\end{aligned}$$

where k is greatest such that $x^{1/k} \ge 2$, i.e., $k = \lfloor \log_2 x \rfloor$

$$\begin{aligned}&< \theta(x) + \log_2 x \, \theta(x^{1/2}) \\ &< \theta(x) + 2x^{1/2} \log x + O(\log^2 x), \qquad \text{using Prop. 9.3.}\end{aligned}$$

□

Curious note: this k is the same one as in the proof of Prop. 9.3, though they have apparently different definitions.

We can now prove

Proposition 9.5. *We have* $\theta(x) \ge x \log 2 + O(x^{1/2} \log x)$.

Proof. Consider the polynomial $p(t) = (t(1-t))^n$ on the interval $[0, 1]$. As $t(1-t) \le \frac{1}{4}$ on that interval (calculus!), we have

$$0 \le p(t) \le \frac{1}{4^n} \qquad \text{on } [0, 1].$$

Writing $p(t) = \sum_{k=0}^{2n} a_k t^k \in \mathbb{Z}[t]$, then

$$\frac{1}{4^n} \ge \int_0^1 p(t) dt = \sum_{k=0}^{2n} \frac{a_k}{k+1} = \frac{N}{d_{2n+1}} \ge \frac{1}{d_{2n+1}},$$

for some $N \in \mathbb{N}$, on putting the fractions over a common denominator. Hence we have successively

$$\begin{aligned} d_{2n+1} &\ge 4^n \\ \psi(2n+1) &\ge 2n \log 2 \qquad \text{on taking logs} \\ \theta(2n+1) &\ge 2n \log 2 - 2 \log(2n+1)\sqrt{2n+1} \qquad \text{by Lemma 9.4} \\ \theta(x) &\ge x \log 2 + O(x^{1/2} \log x).\end{aligned}$$

□

Combining Propositions 9.3 and 9.5, we certainly obtain Theorem 9.2.

9.3. **Some standard estimates.**

Lemma 9.6. *For $t > -1$ we have $\log(1+t) \le t$, with equality iff $t = 0$.*
For $n \in \mathbb{N}$ we have $n \log(1 + \frac{1}{n}) < 1$.

Proof. The first inequality comes from observing that the tangent $y = t$ to the graph of $y = \log(1+t)$ at $t = 0$ lies above the graph, touching it only at $t = 0$. The second inequality comes from putting $t = 1/n$ in the first inequality. □

Lemma 9.7 (Weak Stirling Formula)**.** *For $n \in \mathbb{N}$ we have*

$$n \log n - n < \log(n!) \le n \log n.$$

Proof. Now for $j \ge 2$ we have

$$\begin{aligned} \log j &= j \log j - (j-1)\log(j-1) - (j-1)\log\left(1 + \frac{1}{j-1}\right) \\ &= j \log j - (j-1)\log(j-1) - \delta_j, \end{aligned}$$

where $0 < \delta_j < 1$, using Lemma 9.6 for $n = j - 1$. So, on summing for $j = 2, \dots, n$ we get

$$\begin{aligned} \log(n!) &= \sum_{j=2}^{n} \log j \\ &= \sum_{j=2}^{n} j \log j - (j-1)\log(j-1) - \delta_j \\ &= n \log n - \sum_{j=2}^{n} \delta_j \\ &= n \log n - \Delta, \end{aligned}$$

where $0 < \Delta < n$, since $1 \log 1 = 0$ and all the other $j \log j$ terms apart from $n \log n$ telescope. □

Proposition 9.8. *We have*

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right),$$

where $\gamma = 0.577\dots$, the Euler-Mascheroni constant.

Proof. Draw the graph of $y = 1/t$ for t from $0+$ to $N+1$, where $N = \lfloor x \rfloor$. On each interval $[n, n+1]$ draw a rectangle of height $1/n$, so that these rectangles for $n = 1, 2, \dots, N$ completely cover the area under the curve from $t = 1$ to $t = N + 1$. The pie-shaped pieces of the rectangles above the curve, when moved to the left to lie above the interval $[0, 1]$, are

non-intersecting, and more than half-fill the 1×1 square on that interval. Say their total area is γ_n. Then, as $n \to \infty$, γ_n clearly tends to a limit γ, the Euler-Mascheroni constant.

The sum of the areas of the rectangles above $[n, n+1]$ for $n = 1, 2, \ldots, N$ is clearly $\sum_{n=1}^{N} 1/n$ (the total area of the parts of the rectangles below the curve). On the other hand, it is $\int_1^{N+1} \frac{dx}{x} = \log(N+1)$ (the total area of the parts of the rectangles below the curve), plus γ_n (the total area of the parts of the rectangles above the curve). Hence

$$\sum_{n \le x} \frac{1}{n} = \sum_{n=1}^{N} 1/n = \log(N+1) + \gamma_n.$$

Since $\log(N+1) - \log x = O\left(\frac{1}{x}\right)$ and $\gamma - \gamma_n = O\left(\frac{1}{x}\right)$ (check!), we have the result. □

9.4. **More estimates of sums of functions over primes.** Let us put $\mathcal{P}_x = \prod_{p \le x} \frac{1}{1-p^{-1}}$. Then

Proposition 9.9. *We have $\mathcal{P}_x > \log x$.*

Proof. We have

$$\mathcal{P}_x = \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^n} + \ldots\right).$$

On multiplying these series together, we obtain a sum of terms that includes all fractions $\frac{1}{n}$, where $n \le x$. This is simply because all prime factors of such n are at most x. Hence

$$\mathcal{P}_x > \sum_{n \le x} \frac{1}{n} > \log x,$$

by Prop. 9.8. □

Corollary 9.10. *There are infinitely many primes.*

Proposition 9.11. *We have*

$$\sum_{p \le x} \frac{1}{p} > \log\log x - 1.$$

Proof. We have

$$\begin{aligned} \log \mathcal{P}_x &= \sum_{p \le x} \log\left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^k} + \ldots\right) \\ &< \sum_{p \le x} \frac{1}{p} + \sum_{p \le x} \frac{1}{p(p-1)}, \end{aligned}$$

on applying Lemma 9.6 with $t = \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^k} + \ldots$, and summing the GP, starting with the $1/p^2$ term,

$$\begin{aligned} &< \sum_{p \le x} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{(n+1)n} \\ &= \sum_{p \le x} \frac{1}{p} + \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1} \right) \\ &= \sum_{p \le x} \frac{1}{p} + 1, \end{aligned}$$

because of the telescoping of $\sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1} \right)$. Hence

$$\sum_{p \le x} \frac{1}{p} > \log \mathcal{P}_x - 1 > \log \log x - 1,$$

using Prop. 9.9. □

Proposition 9.12. *We have*

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1) \qquad \text{as } x \to \infty.$$

Proof. Now from Problem Sheet 1, Q8, we have

$$n! = \prod_{p \le n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots},$$

so that (taking logs)

$$\begin{aligned} \log(n!) &= \sum_{p \le n} \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots \right) \log p \\ &= \sum_{p \le n} \left\lfloor \frac{n}{p} \right\rfloor \log p + S_n, \end{aligned}$$

where

$$\begin{aligned} S_n :&= \sum_{p\le n}\left(\left\lfloor\frac{n}{p^2}\right\rfloor+\left\lfloor\frac{n}{p^3}\right\rfloor+\dots\right)\log p \\ &\le \sum_{p\le n}\left(\frac{n}{p^2}+\frac{n}{p^3}+\dots\right)\log p \\ &= n\sum_{p\le n}\frac{\log p}{p(p-1)} \\ &< n\sum_{k=1}^{\infty}\frac{\log(k+1)}{(k+1)k} \\ &= nc, \end{aligned}$$

for some positive constant c, since the last sum is convergent. Hence $nc > S_n > 0$. Also, for $n = \lfloor x \rfloor$ we have

$$\begin{aligned} n\sum_{p\le x}\frac{\log p}{p} &\ge \sum_{p\le x}\left\lfloor\frac{n}{p}\right\rfloor\log p \\ &> \sum_{p\le x}\left(\frac{n}{p}-1\right)\log p \\ &= n\sum_{p\le x}\frac{\log p}{p}-\theta(x). \end{aligned}$$

Hence

$$n\sum_{p\le x}\frac{\log p}{p}\ge\sum_{p\le x}\left\lfloor\frac{n}{p}\right\rfloor\log p > n\sum_{p\le x}\frac{\log p}{p}-O(x),$$

since $\theta(x) = O(x)$, by Theorem 9.2. Now add the inequality $nc > S_n > 0$ to the above inequality, to obtain

$$n\sum_{p\le x}\frac{\log p}{p}+nc > \log(n!) > n\sum_{p\le x}\frac{\log p}{p}-O(x).$$

Dividing by n, and using the fact that $\frac{\log(n!)}{n} = \log n - O(1)$ from Prop. 9.7, we have

$$\sum_{p\le x}\frac{\log p}{p}+O\left(1\right) > \log n - O\left(1\right) > \sum_{p\le x}\frac{\log p}{p}-O\left(1\right).$$

Hence

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1).$$

□

9.5. **The average size of the divisor function $\tau(n)$.** The following result is a way of saying that an integer n has $\log n + 2\gamma - 1$ divisors, on average. Recall that $\tau(n)$ is the number of (positive) divisors of n.

Proposition 9.13. *We have, as $x \to \infty$, that*

$$\sum_{n\le x} \tau(n) = x\log x + (2\gamma-1)x + O\left(\sqrt{x}\right).$$

Proof. Now

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{\ell\mid n} 1\\ &= \sum_{\ell\le x}\sum_{\substack{n=k\ell\\ k\le \frac{x}{\ell}}} 1\\ &= \sum_{\ell\le x}\left\lfloor\frac{x}{\ell}\right\rfloor,\end{aligned}$$

on recalling that $\lfloor y\rfloor$ is the number of positive integers $\le y$,

$$\begin{aligned}&= 2\sum_{\ell\le\sqrt{x}}\left\lfloor\frac{x}{\ell}\right\rfloor - \left\lfloor\sqrt{x}\right\rfloor^2 && \text{by Q10, Problem Sheet 1}\\ &= 2\sum_{\ell\le\sqrt{x}}\frac{x}{\ell} - x + O(\sqrt{x})\\ &= 2x\left(\log\sqrt{x}+\gamma+O\left(\frac{1}{\sqrt{x}}\right)\right) - x + O(\sqrt{x}) && \text{using Prop. 9.8}\\ &= x\log x + (2\gamma-1)x + O(\sqrt{x}).\end{aligned}$$

□