Mathematics 4: Number Theory   Problem Sheet 3

Workshop 26 Oct 2012

The aim of this workshop is to show that Carmichael numbers are squarefree and have at least 3 distinct prime factors.

(1) (Warm-up question.) Show that $n > 1$ is prime iff $a^{n-1} \equiv 1 \pmod{n}$ for $1 \leq a \leq n-1$.

Recall that a positive integer is said to be *squarefree* if it is not divisible by the square of any prime number.

Recall too that a *Carmichael number* is a composite number n with the property that for every integer a coprime to n we have $a^{n-1} \equiv 1 \pmod{n}$.

(2) *Proving that Carmichael numbers are squarefree.*

(a) Show that a given nonsquarefree number n can be written in the form $n = p^\ell N$ for some prime p and integers N and ℓ with $\ell \geq 2$ and $\gcd(p, N) = 1$.

(b) Show that $(1 + pN)^{n-1} \not\equiv 1 \pmod{p^2}$.

(c) Deduce that Carmichael numbers are squarefree.

(3) *Proving that Carmichael numbers have at least 3 distinct prime factors.*

(a) Let p and q be distinct primes. Prove that if $\gcd(a, pq) = 1$ then $a^{\mathrm{lcm}(p-1,q-1)} \equiv 1 \pmod{pq}$.

(b) Now let g be a primitive root $\pmod{p}$ and h be a primitive root $\pmod{q}$. Using g and h, apply the Chinese Remainder Theorem to specify an integer a whose order $\pmod{pq}$ is (exactly) $\mathrm{lcm}(p-1, q-1)$.

(c) Now suppose that p is the larger of the primes p and q.
Calculate $pq - 1 \pmod{p-1} \in \{0, 1, \ldots, p-2\}$.
Deduce that $p - 1 \nmid pq - 1$.

(d) Use the above to show that there is an a with $\gcd(a, pq) = 1$ and $a^{pq-1} \not\equiv 1 \pmod{pq}$.

(e) Deduce from the above that a Carmichael number must have at least 3 distinct prime factors.

(4) (Cool-down question.) Suppose that $a, k, \ell, m, n \in \mathbb{N}$ with $a^k \equiv 1 \pmod{m}$ and $a^\ell \equiv 1 \pmod{n}$. Prove that

(a) $a^{\mathrm{lcm}(k,\ell)} \equiv 1 \pmod{\mathrm{lcm}(m, n)}$;

(b) $a^{\gcd(k,\ell)} \equiv 1 \pmod{\gcd(m, n)}$.

Handin: due Friday, week 7, 2 Nov, before 12.10 lecture. Please hand it in at the lecture

The squarefree part of n

You are expected to write clearly and legibly, giving thought to the presentation of your answer as a document written in mathematical English.

(5) (a) Show that every positive integer n can be written uniquely in the form $n = n_1 n_2^2$, where n_1 is squarefree.
Let us denote n_1 by $g(n)$, the *squarefree part of* n.
(b) Prove that $g(n)$ is a multiplicative function.
(c) Find the Euler product for $D_g(s)$.
(d) Prove that $D_g(s) = \zeta(2s)\zeta(s-1)/\zeta(2s-2)$.

Problems on congruences

(6) Let $m_1, \ldots, m_n$ be pairwise relatively prime. Show that as x runs through the integers $x = 1, 2, 3, \ldots, m_1 m_2 \cdots m_n$, the n-tuples $(x \mod m_1, x \mod m_2, \ldots, x \mod m_n)$ run through all n-tuples in $\prod_{i=1}^{n} \{0, 1, \ldots, m_i - 1\}$.

(7) Show that the equation $x^y \equiv 2 \pmod{19}$ has a solution in integers $\{x, y\}$ iff x is congruent to a primitive root $\mod 19$. Deduce that then y is uniquely specified mod 18.

(8) *Wilson's Theorem.* This states that, for a prime p, we have $(p-1)! \equiv -1 \pmod{p}$.
Prove Wilson's Theorem in (at least!) two different ways.
[Suggestions: (i) Factorize $x^{p-1} - 1$ over $\mathbb{F}_p$. (ii) Try to pair up $a \in \{1, \ldots, p-1\}$ with its multiplicative inverse.]

(9) (a) Find a primitive root for the prime 23.
(b) How many such primitive roots are there?
(c) Find them all.
(d) Find all the quadratic residues and all the quadratic non-residues $\mod 23$.

(10) Solve the equation $x^6 = 7$ in $\mathbb{F}_{19}$, i.e. the equation $x^6 \equiv 7 \pmod{19}$ for $x \in \{0, 1, \ldots, 18\}$.

(11) (a) Let an integer $n > 1$ be given, and let p be its smallest prime factor. Show that there can be at most $p - 1$ consecutive positive integers coprime to n.
(b) Show further that the number $p - 1$ in (a) cannot be decreased, by exhibiting $p - 1$ consecutive positive integers coprime n.
(c) What is $\gcd(p-1, n)$?
(d) Show that $2^n \not\equiv 1 \pmod{n}$.

Problems on arithmetic functions

(12) (a) Let a divisor d of n be given. Among the integers $k = 1, 2, \ldots, n$ show that $\varphi(n/d)$ of them have $\gcd(k, n) = d$.
(b) Deduce that $\sum_{d|n} \varphi(d) = n$.
(c) Deduce that $\varphi(n) = \sum_{d|n} d\mu(n/d)$.

(13) (a) Prove that $\sum_{d|n} \mu(d) = \Delta(n)$, the 1-detecting function.
(b) Let g be any function $\mathbb{R}_{\geq 0} \to \mathbb{R}$, and put $G(x) = \sum_{n \leq x} g(x/n)$, the sum being taken over all positive integers $n \leq x$. Prove that if $x \geq 1$ then $g(x) = \sum_{n \leq x} \mu(n) G(x/n)$.

(14) (a) For which integers n is $\tau(n)$ odd? Here $\tau(n)$ is the number of (positive) divisors of n.
(b) Prove that $\sum_{k|n} \tau(k)^3 = \left(\sum_{k|n} \tau(k)\right)^2$.
[Note that both sides of the equation are multiplicative functions of n.]

(15) (a) An arithmetic function $f(n)$ is said to be *strongly multiplicative* if $f(nm) = f(n)f(m)$ for all $n, m \in \mathbb{N}$. Show that a strongly multiplicative function is completely determined by its values at primes.
(b) Show that if $f(n)$ is a strongly multiplicative function then the Euler product of its Dirichlet function $D_f(s)$ is of the form $\prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}$.

(16) *Strengthening Euler's Theorem.* Suppose that n factorizes as $n = p_1^{f_1} \cdots p_k^{f_k}$. Show that then, for $\gcd(a, n) = 1$, $a^N = 1 \pmod{n}$, where

$$N = \operatorname{lcm}(p_1^{f_1} - p_1^{f_1 - 1}, p_2^{f_2} - p_2^{f_2 - 1}, \ldots, p_k^{f_k} - p_k^{f_k - 1}).$$

For which n is this result no stronger than Euler's theorem $a^{\varphi(n)} = 1 \pmod{n}$?

(17) For two arithmetic functions $A(n)$ and $B(n)$ show that

$$\sum_{d|n} A(d)B(n/d) = \sum_{d|n} A(n/d)B(d).$$

(18) (a) Find the Euler product for $D_{|\mu|}(s) = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s}$.
(b) Prove that $D_{|\mu|}(s) = \zeta(s)/\zeta(2s)$.

(19) Let $\omega(n)$ denote the number of prime factors of n. Show that the function $e^{\omega(n)}$ is a multiplicative function.

(20) Let f be any arithmetic function.
(a) Show that $\sum_{n \leq x} \sum_{k|n} f(k) = \sum_{n \leq x} f(n) \left\lfloor \frac{x}{n} \right\rfloor$.

(b) Now put $F(x) = \sum_{n \le x} f(n)$. Deduce that $\sum_{n \le x} f(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n \le x} F\left(\frac{x}{n}\right)$.

(21) (a) Prove that for $x \ge 1$ we have $\sum_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1$.
(b) (Harder) Deduce that for all $x \ge 1$ we have

$$\left| \sum_{n \le x} \frac{\mu(n)}{n} \right| \le 1.$$

(22) The Dirichlet series $D_f(s)$ of a certain arithmetic function $f(n)$ has Euler product $\prod_p \left(1 - \frac{1}{p^s} + \frac{1}{p^{2s}}\right)$.
(a) Show that $f(n) \ne 0$ iff n is "cube-free", and give a precise definition of this term.
(b) Find an explicit description of $f(n)$.
(c) Find the Euler product for $D_{|f|}(s) = \sum_{n=1}^{\infty} \frac{|f(n)|}{n^s}$.
(d) Prove that $D_{|f|}(2s) = D_{|f|}(s) D_f(s)$.

Problems around primality testing

(23) *Fast exponentiation: Computing a^r by the SX method.*

Let $a \in \mathbb{Z}, r \in \mathbb{N}$. Write r in binary as $r = b_k b_{k-1} \cdots b_1 b_0$, with all $b_i \in \{0, 1\}$. From the binary string $b_k b_{k-1} \cdots b_1 b_0$ produce a string of S's and X's by replacing each 0 by S and each 1 by SX. Now, starting with $A = 1$ and working from left to right, interpret S as $A \to A^2$ (i.e. replace A by A^2), and X as $A \to Aa$ (multiply A by a).

Prove that the result of this algorithm is indeed a^r.

[This algorithm is particularly useful for exponentiation (mod n), but it works for any associative multiplication on any set. Note that the leading S does nothing, so can be omitted.]

(24) Compute $2^{90} \pmod{91}$ by the SX method. What does this tell you about 91?
[Maple: `convert(n,binary);`]

(25) (a) Show that if n is not a pseudoprime to base bb' where $\gcd(b, b') = 1$ then it is not a pseudoprime either to base b or to base b'.

(b) Show that if n is not a pseudoprime to base b^k where $k > 1$ then it is not a pseudoprime to base b.
[Thus it's always enough to use the pseudoprime test with prime bases.]
(c) Repeat (a) and (b) with 'pseudoprime' replaced by 'strong pseudoprime'.

(26) Show that the Carmichael number 561 is not a strong pseudoprime to base 2, but that 2047 is. Show, however, that 2047 is not a strong pseudoprime to base 3.
[Useful Maple: `with(numtheory);?phi,?mod`]

(27) (a) Prove that if $6k+1, 12k+1$ and $18k+1$ are all prime, then their product is a Carmichael number. [Use Q 16]

(b) Show that the first few values of k for which (a) gives Carmichael numbers are $k = 1, 6, 35, 45, \ldots$. What is the next such value of k?
[This is the integer sequence A046025– via "integer sequences", found e.g., by Google]
[Maple `?isprime`]