Mathematics 4: Number Theory Problem Sheet 4

Workshop 9 Nov 2012

Working with quadratic residues and primitive roots

(1) Given an odd prime p with g a primitive root $\pmod p$, which powers of g are:
   (a) quadratic residues?
   (b) primitive roots?
   (Just need to refer to results from notes.)

(2) For $p = 3, 5, 7$ and 11:
   (a) find a primitive root;
   (b) work out which of $1, 2, \ldots, p-1$ are
      - quadratic residues;
      - primitive roots;
      - neither.

(3) Evaluate $\left(\frac{-2}{p}\right)$ for odd primes p. When is $p-2$ a quadratic residue?

(4) Show that if $p = 8n-1$ and $q = 4n-1$ are both primes, then $(-2)^q \equiv -1 \pmod p$. Deduce that -2 is a primitive root $\pmod p$.

Now recall (special case of Q 4(b), Problem Sheet 3)) that if $a^k \equiv 1 \pmod p$ and $a^\ell \equiv 1 \pmod p$ then $a^{\gcd(k,\ell)} \equiv 1 \pmod p$.

(5) *Prime factors of M_p are large.* Let p be an odd prime, and q be a prime factor of $M_p = 2^p - 1$.
   (a) Show that
   $$2^{\gcd(p,q-1)} \equiv 1 \pmod q.$$
   Deduce that $p \mid (q-1)$, and hence that $q = 2rp + 1$ for some $r \in \mathbb{N}$.
   (b) Find the prime factors of M_{11}.
   (c) If M_p is in fact prime, what is r?

Handin: due Friday, week 9, 16 Nov, before 12.10 lecture. Please hand it in at the lecture

Prime factors of Fermat numbers are large

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

(6) Let $k \in \mathbb{N}$ and q be a prime factor of $F_k = 2^{2^k} + 1$.
   (a) Show that $2^{2^k} \equiv -1 \pmod{q}$, and that $2^{2^\ell} \not\equiv 1 \pmod{q}$ for $\ell = 1, 2, \ldots, k$.
   (b) Show that
   $$2^{\gcd(q-1, 2^{k+1})} \equiv 1 \pmod{q}.$$
   (c) Deduce that $\gcd(q-1, 2^{k+1}) = 2^{k+1}$, and that $q = 2^{k+1}r + 1$ for some $r \in \mathbb{N}$.
   (d) Use this to find a prime factor of F_5.

Further quadratic residues and primitive root problems

(7) Calculate the Legendre symbols (a) $\left(\frac{23}{31}\right)$, (b) $\left(\frac{211}{307}\right)$ (c) $\left(\frac{2053}{3061}\right)$ using the law of quadratic reciprocity. Check your answer with Maple. [`with(numtheory): legendre`]

(8) If n is the product of k distinct odd primes, show that the congruence $x^2 \equiv 1 \pmod{n}$ has 2^k different solutions.

(9) Prove that, for p an odd prime, $\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$.

(10) Let p be an odd prime, and suppose that the set $\{1, 2, \ldots, p-1\}$ is partitioned into two nonempty sets $\mathcal{S}_1$ and $\mathcal{S}_2$ such that the product $\pmod{p}$ of any two elements in the same set is in $\mathcal{S}_1$, while the product $\pmod{p}$ of an element in $\mathcal{S}_1$ and an element in $\mathcal{S}_2$ is in $\mathcal{S}_2$. Prove that $\mathcal{S}_1$ is the set of quadratic residues $\pmod{p}$ while $\mathcal{S}_2$ is the set of quadratic nonresidues $\pmod{p}$.

(11) Show that if $2^n - 1$ is prime, then n is prime.

(12) Show that if $2^n + 1$ is prime, then n is a power of 2.

(13) Show that, for $n > 1$, 3 is a primitive root of any prime of the form $2^n + 1$.

Sums of Squares Problems

Throughout, 'squares' will mean ' squares of integers', unless otherwise stated.

(14) Show that a positive integer n is a sum of two squares iff n^3 is the sum of two squares.

Which exponents can replace '3' in this result and have it remain true?

(15) *Representing n as the difference of two squares.*
   (a) Show that a square is $\equiv 0$ or $1 \pmod 4$.
   (b) Show that if $n \equiv 2 \pmod 4$ then it is not a difference of two squares.
   (c) With the help of $(n+1)^2 - n^2$ and $(n+1)^2 - (n-1)^2$, prove that all integers except those in (b) can be written as the difference of two squares.

(16) Show that if an odd number n is the sum of two squares then $n \equiv 1 \pmod 4$.

(17) Show that a positive integer n can be written as $n = x^2 + 4y^2$ iff n is the sum of two squares and also n is not twice an odd number.

(18) Which integers can be written as the difference of two *nonzero* squares?

(19) Show that every integer can be written as the difference of two squares of rationals.

(20) Show that every integer can be written as $x^2 - y^2 + z^2$ for some integers x, y, z.

(21) *Representing primes as $x^2 + 2y^2$.*
   (a) Show that, for an odd prime p, $\left(\frac{-2}{p}\right) = 1$ iff $p \equiv 1$ or $3 \pmod 8$.
   (b) Show that if an odd prime p can be written as $p = x^2 + 2y^2$, then $p \equiv 1$ or $3 \pmod 8$.
   (c) Conversely, following the proof of Th. 6.1 (which was for $p = x^2 + y^2$), show that, for p a prime with $p \equiv 1$ or $3 \pmod 8$ there are positive integers x, y with $x^2 + 2y^2 = p$ or $= 2p$.
   (d) Show how a solution of $x^2 + 2y^2 = 2p$ gives rise to a solution of $x^2 + 2y^2 = p$, so that a prime $p \equiv 1$ or $3 \pmod 8$ always has a representation $p = x^2 + 2y^2$.

(22) *Representing primes as $x^2 + 3y^2$.*
   (a) Show that, for a prime $p > 3$, $\left(\frac{-3}{p}\right) = 1$ iff $p \equiv 1 \pmod 6$. [Work mod 12.]
   (b) Show that if a prime $p > 3$ can be written as $p = x^2 + 3y^2$, then $p \equiv 1 \pmod 6$.

(c) Conversely, following the proof of Th. 6.1, show that, for p a prime with $p \equiv 1 \pmod 6$ there are positive integers x, y with $x^2 + 3y^2 = p$ or $= 2p$ or $= 3p$.
(d) Show that the case $x^2 + 3y^2 = 2p$ in (c) cannot occur, so that $x^2 + 3y^2 = p$ or $= 3p$.
(e) Show how a solution of $x^2 + 3y^2 = 3p$ gives rise to a solution of $x^2 + 3y^2 = p$, so that a prime $p \equiv 1 \pmod 6$ always has a representation $p = x^2 + 3y^2$.

Miscellaneous Problems

(23) Prove Wolstenholme's theorem: if p is a prime greater than 3 then the numerator of the fraction

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p^2.

(24) Suppose that $a, b, c > 1$ with $ab \equiv 1 \pmod c, bc \equiv 1 \pmod a$ and $ca \equiv 1 \pmod b$. Prove that $\{a, b, c\} = \{2, 3, 5\}$.

(25) Let n be a positive integer. How many digits has n? What is its most significant digit? Its least significant digit?
Assuming n has an odd number of digits, what is its middle digit?
[The functions $\lfloor \quad \rfloor$ and $\log_{10}$ may be useful for this question.]

(26) *Cunningham chains.* A sequence $p_1, p_2, \ldots, p_k$ of primes is called a *Cunningham chain* if $p_{i+1} = 2p_i + 1$ for $i = 1, \ldots, k-1$, and neither $(p_1 - 1)/2$ nor $2p_k + 1$ are prime numbers.
(a) Find the Cunningham chain with $p_1 = 2$.
(b) Show that any Cunningham chain containing any prime $\not\equiv 9 \pmod{10}$ must either be the chain in (a), or have length at most 3. Give an example of the latter.
(c) Deduce that any Cunningham chain of length 4 or more, apart from that in (a), must have every prime $\equiv 9 \pmod{10}$.
(d) Show that $p_i = 2^{i-1}(p_1 + 1) - 1$ for $i = 1, \ldots, k$.
(e) Now take $p_1 > 2$. Show that then p_1 divides p_{p_1}, and that $k < p_1$.
(f) Check that the Cunningham chain with $p_1 = 2759832934171386593519$ has length 17. [Maple: `isprime`]