MAS/320 Number Theory: Coursework 5

Franco VIVALDI

http://www.maths.qmw.ac.uk/~fv/teaching/nt/nt.html

This coursework will be assessed and count towards your final mark for the course

DEADLINE: Wednesday of week 12, at 1:00 pm.

CONTENT: Modular arithmetic.

M⋆icroESSAY: Write an essay on quadratic residues. (Approximately 100 words, and no mathematical symbols.)

Problem 1. Construct a reduced residue system modulo 15 consisting entirely of (a) prime numbers; (b) composite numbers.

Problem 2. Calculate $\phi(m)$ for the following values of m

a) 512; *b*) 1155; *c*) 10!.

Problem 3. Let $\Psi(n) = \phi(n)/n$, for $n \geq 1$.

(a) Show that the value of $\Psi(n)$ depends only on the prime divisors of n.

(b) Find the least n such that $\Psi(n) < 1/4$.

(c) Construct an infinite sequence n_k of positive integers for which $\phi(n_k) < n_k/5$, whence determine an integer $n > 10^6$ with the same property. Such n should be as small as possible, and in any case smaller than $2 \cdot 10^6$.

Problem 4. In each case, construct the set of positive integers m with the stated property.

a) $\phi(m) \not\equiv 0 \pmod 4$; *b*) $\phi(m) \mid m$.

Problem 5. For the following values of m find all primitive roots modulo m

a) 13; *b*) 23; *c*) 26.

Problem 6. Compute the quantity

$$\frac{7}{13} \pmod{23}$$

in two ways:

(a) Determine $1/13$ by solving $x \cdot 13 \equiv 1 \pmod{23}$, using continued fractions.

(b) Determine $1/13$ as $13^{-1} = 13^{t-1}$, where t is the order of 13 modulo 23.

Problem 7*. Let $r = p/q$ be a rational number, with p and q coprime, and q coprime to 10. It can be shown that the decimal digits of r are periodic. Prove that the length of the period is equal to the order of 10 modulo q.

Problem 8. Compute the value of the following Legendre symbols

$$a)\ \left(\frac{43}{59}\right); \qquad b)\ \left(\frac{35}{113}\right); \qquad c)\ \left(\frac{365}{1847}\right).$$

Problem 9. Let p be a prime > 3. Show that

$$(3/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Problem 10. Prove that the product of the quadratic residues of p is congruent to $(-1)^{(p+1)/2}$ modulo p. [*Hint:* use a primitive root.]

Problem 11. Prove that if p is an odd prime and $\gcd(a,p) = 1$, we have

$$\sum_{k=1}^{p-1} \left(\frac{ka}{p}\right) = 0.$$

[*Hint:* use a primitive root.]

Problem 12*. Show that if p and $q = 4p + 1$ are both primes, then 2 is a primitive root modulo q.