II(C) Number Theory — Key Questions

July 2012 *V. Neale*

These questions are designed to expand on the information in the Schedules, to help you prepare for the course over the summer. They are the questions that a student who takes the Number Theory course should expect to be able to answer at the end of the course. You might like to try tackling the questions yourself; you might like to use them to guide your reading; or you might like to do a mixture of the two. They are not problems like those found on examples sheets, but rather are the key questions that the lectures will seek to answer.

The questions appear in the order in which the topics appear in the Schedules, but this may not be the order in which the lecturer covers the material. The relevant parts of the Schedules are quoted at appropriate points.

Review from Part IA Numbers and Sets: Euclid's Algorithm, prime numbers, fundamental theorem of arithmetic. Congruences. The theorems of Fermat and Euler. [2]

- This is material that was covered in IA. You could refresh your memory by thinking about how you would present it to someone who has not seen it before.

Chinese remainder theorem. Lagrange's theorem. Primitive roots to an odd prime power modulus. [3]

The *multiplicative group* modulo n is the group of units (invertible elements) under multiplication, and is often denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$.

- What does the Chinese remainder theorem tell us about the structure of the groups $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ for various n?
- Let p be a prime and let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, where a_n is not divisible by p. How many roots can f have modulo p? (That is, how many solutions are there to the congruence $f(x) \equiv 0 \pmod{p}$?)
- Let p be an odd prime and let j be a natural number. What is the structure of the group $(\mathbb{Z}/p^j\mathbb{Z})^\times$?

The mod-p field, quadratic residues and non-residues, Legendre's symbol. Euler's criterion. Gauss' lemma, quadratic reciprocity. [2]

Let a be an integer coprime to the integer n. Then we say that a is a *quadratic residue* modulo n if there is a solution to the congruence $x^2 \equiv a \pmod{n}$, and a *quadratic non-residue* if there is not a solution to that congruence. For a prime p, the *Legendre symbol* is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } (a,p) > 1. \end{cases}$$

- Let p be a prime. How many quadratic residues are there modulo p? (For example, there are three quadratic residues modulo 7.)
- Let p be a prime, and let a be coprime to p. Why must $a^{(p-1)/2}$ be congruent to ± 1 modulo p? Which a give $+1$, and which give -1?
- For which primes p is -1 a quadratic residue?

- For which primes p is 2 a quadratic residue?
- Let p and q be two odd primes. What is the relationship between the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$?

Proof of the law of quadratic reciprocity. The Jacobi symbol. [1]

Let n be a natural number greater than 1, with prime factorisation $n = p_1^{e_1} \cdots p_k^{e_k}$. The *Jacobi symbol* is defined to be

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

- Is is the case that $\left(\frac{a}{n}\right) = 1$ if and only if a is a quadratic residue modulo n?
- Which of the results that hold for the Legendre symbol also hold for the Jacobi symbol?

Binary quadratic forms. Discriminants. Standard form. Representation of primes. [5]

A *binary quadratic form* is an object of the form $ax^2+bxy+cy^2$, where the coefficients a, b and c are integers (and we think of x and y as integer variables).

- What is the link between binary quadratic forms $ax^2+bxy+cy^2$ and 2×2 integer matrices with determinant 1?
- When do two forms represent the same set of numbers?
- What does it mean to say that two binary quadratic forms are *equivalent*? How can we choose a representative of each equivalence class? (These representatives are known as *reduced* forms.)
- Which numbers can be represented by a specific positive definite form $ax^2 + bxy + cy^2$ (one where $a > 0$ and $b^2 - 4ac < 0$)?
- Which numbers are represented by the form $x^2 + y^2$? That is, which numbers can be written as a sum of two squares?

Distribution of the primes. Divergence of $\sum_p p^{-1}$. The Riemann zeta-function and Dirichlet series. Statement of the prime number theorem and of Dirichlet's theorem on primes in an arithmetic progression. Legendre's formula. Bertrand's postulate. [4]

The Riemann zeta function is defined for complex numbers s with $\Re(s) > 1$ by $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

We define $\pi(x)$ to be the number of primes up to x: that is, we define $\pi(x) = \#\{p : p \text{ prime and } p \leq x\}$.

- How does $\sum_{p\leq x} \frac{1}{p}$ grow as a function of x? (The sum is over all primes up to x.)
- How is the Riemann zeta function related to the primes? Prove the *Euler product*: if $\Re(s) > 1$, then $\zeta(s) = \prod_p (1-p^{-s})^{-1}$ (where the product is over all primes p).
- How does $\pi(x)$ grow as a function of x? How does the Riemann zeta function help to prove the Prime Number Theorem? (Note: the Prime Number Theorem is not proved in this course, although the lecturer may give a sketch proof.)
- Under what circumstances are there infinitely many primes in the arithmetic progression a, $a + n$, $a + 2n$, ...? That is, for which a and n are there infinitely

many primes congruent to a modulo n? (Note: Dirichlet's theorem on primes in arithmetic progressions is not proved in this course.)
- How can we use the inclusion-exclusion principle to find $\pi(x)$ (perhaps in terms of $\pi(\sqrt{x})$ amongst other things)?
- Is there always a prime between n and $2n$?

Continued fractions. Pell's equation. [3]

The equation $x^2 - Ny^2 = 1$ (where N is not a square) is known as Pell's equation.

- What is the relationship between Euclid's algorithm and continued fractions for rational numbers?
- How do continued fractions lead to good rational approximations for real numbers?
- How can we use continued fractions to find integer solutions to Pell's equation?

Primality testing. Fermat, Euler and strong pseudo-primes. [2]

- Fermat's Little Theorem tells us that if p is prime and a is coprime to p, then $a^{p-1} \equiv 1 \pmod{p}$. If we have an integer n and we know that $a^{n-1} \equiv 1 \pmod{n}$ for some a, does that tell us that n is prime? If the congruence is satisfied for *all* a coprime to n, does that imply that n is prime?
- Euler's criterion tells us that if p is prime and a is coprime to p, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. If we have an integer n and we know that $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ for some a, does that tell us that n is prime? If the congruence is satisfied for *all* a coprime to n, does that imply that n is prime?
- Prove that if p is prime and a is coprime to p and $p - 1 = 2^s t$ where t is odd, then either $a^t \equiv 1 \pmod{p}$ or $a^{2^r t} \equiv -1 \pmod{p}$ for some $r \in \{0, 1, \ldots, s-1\}$. If we have an integer n for which this condition is satisfied for some a, does that tell us that n is prime? If the condition is satisfied for *all* a coprime to n, does that imply that n is prime?

Factorization. Fermat factorization, factor bases, the continued-fraction method. Pollard's method. [2]

- Given a large integer N, we want to find a non-trivial factor. Why might it help to find r and s such that $r^2 \equiv s^2 \pmod{N}$? Can we always find such squares?
- How might we find such r and s with the help of a *factor base* B and some suitable B-numbers? How could we use continued fractions to help find such B-numbers?

Please e-mail me with comments, suggestions and queries (v.r.neale@dpmms.cam.ac.uk).