Part II

Number Theory

Year

Paper 1, Section I

1I Number Theory

A function $f:\mathbb{N}\to\mathbb{C}$ is *multiplicative* if $f(mn)=f(m)f(n)$ for all m,n coprime. Show that if f is multiplicative then so is $g(n)=\sum_{d\mid n} f(d)$. Define the *Möbius function* μ and *Euler function* ϕ. Establish the identities

$$\frac{\phi(n)}{n}=\sum_{d\mid n}\frac{\mu(d)}{d} \qquad \text{and} \qquad \frac{n}{\phi(n)}=\sum_{d\mid n}\frac{\mu(d)^2}{\phi(d)}\,.$$

Paper 2, Section I

1I Number Theory

Explain what it means for a positive definite binary quadratic form to be *reduced*, and what it means for two such forms to be *equivalent.* Prove that every positive definite binary quadratic form is equivalent to a reduced form. Show that any two equivalent forms represent the same set of integers.

Carefully quoting any further results you need, show that $f(x,y)=6x^2+5xy+2y^2$ and $g(x,y)=9x^2+25xy+18y^2$ represent the same integers, but are not equivalent.

Paper 3, Section I

1I Number Theory

State *Lagrange's theorem* on the possible number of solutions of a polynomial congruence. State and prove the *Chinese remainder theorem.*

Find the smallest positive integer x satisfying $x^3+1\equiv 0 \pmod{1729}$. Hence, or otherwise, determine the number of solutions of this congruence with $1\leqslant x\leqslant 1729$.

Paper 4, Section I

1I Number Theory

Compute the continued fraction expansion of $\sqrt{29}$.

Find integers x and y satisfying $x^2-29y^2=-1$.

Paper 3, Section II
11I Number Theory

(a) Define what it means for an integer to be a *primitive root* mod n.

(b) Let p be an odd prime, and b a primitive root mod p. Prove the following are equivalent.

(i) b is a primitive root mod p^2.

(ii) b is a primitive root mod p^m for all $m \geqslant 2$.

(iii) No pseudoprime to the base b is divisible by p^2.

(c) Find the three smallest positive integers b with the property that b is a primitive root mod 5^m for all $m \geqslant 1$.

(d) Let $P(n)$ be the number of primitive roots mod n. Show that for each $k \geqslant 1$ there are only finitely many integers n with $P(n) = k$.

Paper 4, Section II
11I Number Theory

(a) Define the *Legendre symbol* and state *Euler's criterion.* State and prove *Gauss' lemma.* Determine the primes p for which the congruence $x^2 \equiv 2 \pmod{p}$ is soluble.

(b) Let $\pi_k(x)$ be the number of primes p less than or equal to x with $p \equiv k \pmod{8}$.

(i) By considering the prime factorisation of $n^2 - 2$ for suitable n, show that $\pi_7(x) \to \infty$ as $x \to \infty$.

(ii) By considering the prime factorisation of $n^2 - 2$ for all n in a suitable range, show that for all x sufficiently large we have

$$\pi_1(x) + \pi_7(x) + 1 \geqslant \frac{\log x}{6 \log 3}\,.$$

Paper 1, Section I

1I Number Theory

State Euler's criterion.

Let p be an odd prime. Show that every primitive root modulo p is a quadratic non-residue modulo p.

Let p be a Fermat prime, that is, a prime of the form $2^{2^k}+1$ for some $k \geqslant 1$. By evaluating $\phi(p-1)$, or otherwise, show that every quadratic non-residue modulo p is a primitive root modulo p. Deduce that 3 is a primitive root modulo p for every Fermat prime p.

Paper 2, Section I

1I Number Theory

Define the *Möbius function* μ, and explain what it means for it to be *multiplicative.*

Show that for every positive integer n

$$\sum_{d|n} \frac{\mu(d)^2}{\phi(d)} = \frac{n}{\phi(n)},$$

where ϕ is the Euler totient function.

Fix an integer $k \geqslant 1$. Use the Chinese remainder theorem to show that there are infinitely many positive integers n for which

$$\mu(n) = \mu(n+1) = \cdots = \mu(n+k).$$

Paper 3, Section I

1I Number Theory

Define the *continued fraction expansion* of $\theta \in \mathbb{R}$, and show that this expansion terminates if and only if $\theta \in \mathbb{Q}$.

Define the *convergents* $(p_n/q_n)_{n \geqslant -1}$ of the continued fraction expansion of θ, and show that for all $n \geqslant 0$,

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}.$$

Deduce that if $\theta \in \mathbb{R} \setminus \mathbb{Q}$, then for all $n \geqslant 0$, at least one of

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{and} \quad \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}$$

must hold.

[You may assume that θ lies strictly between p_n/q_n and p_{n+1}/q_{n+1} for all $n \geqslant 0$.]

Paper 4, Section I
1I Number Theory

Let p be a prime, and let $N = \binom{2n}{n}$ for some positive integer n.

Show that if a prime power p^k divides N for some $k \geqslant 1$, then $p^k \leqslant 2n$.

Given a positive real x, define $\psi(x) = \sum_{n \leqslant x} \Lambda(n)$, where $\Lambda(n)$ is the von Mangoldt function, taking the value $\log p$ if $n = p^k$ for some prime p and integer $k \geqslant 1$, and 0 otherwise. Show that

$$\psi(x) = \sum_{p \leqslant x,\ p \text{ prime}} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Deduce that for all integers $n > 1$, $\psi(2n) \geqslant n \log 2$.

Paper 3, Section II
11I Number Theory

State what it means for two binary quadratic forms to be *equivalent*, and define the *class number* $h(d)$.

Let m be a positive integer, and let f be a binary quadratic form. Show that f properly represents m if and only if f is equivalent to a binary quadratic form

$$mx^2 + bxy + cy^2$$

for some integers b and c.

Let $d < 0$ be an integer such that $d \equiv 0$ or $1 \mod 4$. Show that m is properly represented by some binary quadratic form of discriminant d if and only if d is a square modulo $4m$.

Fix a positive integer $A \geqslant 2$. Show that $n^2 + n + A$ is composite for some integer n such that $0 \leqslant n \leqslant A - 2$ if and only if $d = 1 - 4A$ is a square modulo $4p$ for some prime $p < A$.

Deduce that $h(1-4A) = 1$ if and only if n^2+n+A is prime for all $n = 0, 1, \ldots, A-2$.

Paper 4, Section II

11I Number Theory

(a) Let $N \geqslant 3$ be an odd integer and b an integer with $(b, N) = 1$. What does it mean to say that N is a *(Fermat) pseudoprime to base* b?

Let $b, k \geqslant 2$ be integers. Show that if $N \geqslant 3$ is an odd composite integer dividing $b^k - 1$ and satisfying $N \equiv 1 \mod k$, then N is a pseudoprime to base b.

(b) Fix $b \geqslant 2$. Let p be an odd prime not dividing $b^2 - 1$, and let

$$n = \frac{b^p - 1}{b - 1} \quad \text{and} \quad m = \frac{b^p + 1}{b + 1}.$$

Use the conclusion of part (a) to show that $N = nm$ is a pseudoprime to base b. Deduce that there are infinitely many pseudoprimes to base b.

(c) Let $b, k \geqslant 2$ be integers, and let $n = p_1 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes not dividing $2b$. For each $j = 1, 2, \ldots, k$, let $r_j = n/p_j$. Show that n is a pseudoprime to base b if and only if for all $j = 1, 2, \ldots, k$, the order of b modulo p_j divides $r_j - 1$.

(d) By considering products of prime factors of $2^k - 1$ and $2^k + 1$ for primes $k \geqslant 5$, deduce that there are infinitely many pseudoprimes to base 2 with two prime factors.

[*Hint: You may assume that* $\gcd(j, k) = 1$ *for* $j, k \geqslant 1$ *implies* $\gcd(2^j - 1, 2^k - 1) = 1$, *and that for* $k > 3$, $2^k + 1$ *is not a power of* 3.]

Paper 1, Section I

1H Number Theory

What does it mean to say that a positive definite binary quadratic form is *reduced*?

Find all reduced binary quadratic forms of discriminant -20.

Prove that if a prime $p \neq 5$ is represented by $x^2 + 5y^2$, then $p \equiv 1, 3, 7$ or $9 \mod 20$.

Paper 2, Section I

1H Number Theory

Let $\theta \in \mathbb{R}$.

For each integer $n \geqslant -1$, define the convergents p_n/q_n of the continued fraction expansion of θ. Show that for all $n \geqslant 0$, $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$. Deduce that if $q \in \mathbb{N}$ and $p \in \mathbb{Z}$ satisfy

$$\left|\theta - \frac{p}{q}\right| < \left|\theta - \frac{p_n}{q_n}\right|,$$

then $q > q_n$.

Compute the continued fraction expansion of $\sqrt{12}$. Hence or otherwise find a solution in positive integers x and y to the equation $x^2 - 12y^2 = 1$.

Paper 3, Section I

1H Number Theory

Let $N \geqslant 3$ be an odd integer and b an integer with $(b, N) = 1$. What does it mean to say that N is an *Euler pseudoprime to base* b?

Show that if N is not an Euler pseudoprime to some base b_0, then it is not an Euler pseudoprime to at least half the bases $\{1 \leqslant b < N : (b, N) = 1\}$.

Show that if N is odd and composite, then there exists an integer b such that N is not an Euler pseudoprime to base b.

Paper 4, Section I

1H Number Theory

Let p be a prime.

State and prove Lagrange's theorem on the number of solutions of a polynomial congruence modulo p. Deduce that $(p-1)! \equiv -1 \mod p$.

Let k be a positive integer such that $k|(p-1)$. Show that the congruence

$$x^k \equiv 1 \mod p$$

has precisely k solutions modulo p.

Paper 3, Section II

11H Number Theory

Let p be an odd prime.

(i) Define the *Legendre symbol* $\left(\frac{x}{p}\right)$, and show that when $(x,p)=1$, then $\left(\frac{x^{-1}}{p}\right)=\left(\frac{x}{p}\right)$.

(ii) State and prove Gauss's lemma, and use it to evaluate $\left(\frac{-1}{p}\right)$. [You may assume Euler's criterion.]

(iii) Prove that

$$\sum_{x=1}^{p}\left(\frac{x}{p}\right)=0,$$

and deduce that

$$\sum_{x=1}^{p}\left(\frac{x(x+1)}{p}\right)=-1.$$

Hence or otherwise determine the number of pairs of consecutive integers $z, z+1$ such that $1 \leqslant z, z+1 \leqslant p-1$ and both z and $z+1$ are quadratic residues mod p.

Paper 4, Section II

11H Number Theory

(a) What does it mean to say that a function $f : \mathbb{N} \to \mathbb{C}$ is *multiplicative*? Show that if $f, g : \mathbb{N} \to \mathbb{C}$ are both multiplicative, then so is $f \star g : \mathbb{N} \to \mathbb{C}$, defined for all $n \in \mathbb{N}$ by

$$f \star g(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right).$$

Show that if $f = \mu \star g$, where μ is the Möbius function, then $g = f \star 1$, where 1 denotes the constant function 1.

(b) Let $\tau(n)$ denote the number of positive divisors of n. Find $f, g : \mathbb{N} \to \mathbb{C}$ such that $\tau = f \star g$, and deduce that τ is multiplicative. Hence or otherwise show that for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$,

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta(s)^2,$$

where ζ is the Riemann zeta function.

(c) Fix $k \in \mathbb{N}$. By considering suitable powers of the product of the first $k+1$ primes, show that

$$\tau(n) \geqslant (\log n)^k$$

for infinitely many $n \in \mathbb{N}$.

(d) Fix $\epsilon > 0$. Show that

$$\frac{\tau(n)}{n^\epsilon} = \prod_{p \text{ prime},\, p^\alpha || n} \frac{(\alpha+1)}{p^{\alpha\epsilon}},$$

where $p^\alpha \,||\, n$ denotes the fact that $\alpha \in \mathbb{N}$ is such that $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$. Deduce that there exists a positive constant $C(\epsilon)$ depending only on ϵ such that for all $n \in \mathbb{N}$, $\tau(n) \leqslant C(\epsilon) n^\epsilon$.

Paper 4, Section I

1I Number Theory

Show that the product

$$\prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)^{-1}$$

and the series

$$\sum_{p \text{ prime}} \frac{1}{p}$$

are both divergent.

Paper 3, Section I

1I Number Theory

Let $f=(a,b,c)$ be a positive definite binary quadratic form with integer coefficients. What does it mean to say that f is *reduced*? Show that if f is reduced and has discriminant d, then $|b| \leqslant a \leqslant \sqrt{|d|/3}$ and $b \equiv d \pmod 2$. Deduce that for fixed $d<0$, there are only finitely many reduced f of discriminant d.

Find all reduced positive definite binary quadratic forms of discriminant -15.

Paper 2, Section I

1I Number Theory

Define the *Jacobi symbol* $\left(\frac{a}{n}\right)$, where a, $n \in \mathbb{Z}$ and n is odd and positive.

State and prove the *Law of Quadratic Reciprocity* for the Jacobi symbol. [You may use Quadratic Reciprocity for the Legendre symbol without proof but should state it clearly.]

Compute the Jacobi symbol $\left(\dfrac{503}{2019}\right)$.

Paper 1, Section I

1I Number Theory

(a) State and prove the *Chinese remainder theorem.*

(b) Let N be an odd positive composite integer, and b a positive integer with $(b,N)=1$. What does it mean to say that N is a *Fermat pseudoprime to base b*? Show that 35 is a Fermat pseudoprime to base b if and only if b is congruent to one of 1, 6, 29 or 34 (mod 35).

Paper 4, Section II

11I Number Theory

(a) Let a_0, $a_1, \ldots$ be positive integers, and $\beta > 0$ a positive real number. Show that for every $n \geqslant 0$, if $\theta_n = [a_0, \ldots, a_n, \beta]$, then $\theta_n = (\beta p_n + p_{n-1})/(\beta q_n + q_{n-1})$, where (p_n), (q_n) $(n \geqslant -1)$ are sequences of integers satisfying

$$p_0 = a_0, \ q_0 = 1, \quad p_{-1} = 1, \ q_{-1} = 0 \quad \text{and}$$
$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \quad (n \geqslant 1).$$

Show that $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, and that θ_n lies between p_n/q_n and p_{n-1}/q_{n-1}.

(b) Show that if $[a_0, a_1, \ldots]$ is the continued fraction expansion of a positive irrational θ, then $p_n/q_n \to \theta$ as $n \to \infty$.

(c) Let the convergents of the continued fraction $[a_0, a_1, \ldots, a_n]$ be p_j/q_j $(0 \leqslant j \leqslant n)$. Using part (a) or otherwise, show that the n-th and $(n-1)$-th convergents of $[a_n, a_{n-1}, \ldots, a_0]$ are p_n/p_{n-1} and q_n/q_{n-1} respectively.

(d) Show that if $\theta = [\overline{a_0, a_1, \ldots, a_n}]$ is a purely periodic continued fraction with convergents p_j/q_j, then $f(\theta) = 0$, where $f(X) = q_n X^2 + (q_{n-1} - p_n)X - p_{n-1}$. Deduce that if θ' is the other root of $f(X)$, then $-1/\theta' = [\overline{a_n, a_{n-1}, \ldots, a_0}]$.

Paper 3, Section II

11I Number Theory

Let $p > 2$ be a prime.

(a) What does it mean to say that an integer g is a primitive root mod p?

(b) Let k be an integer with $0 \leqslant k < p-1$. Let

$$S_k = \sum_{x=0}^{p-1} x^k.$$

Show that $S_k \equiv 0 \pmod{p}$. [Recall that by convention $0^0 = 1$.]

(c) Let $f(X,Y,Z) = aX^2 + bY^2 + cZ^2$ for some a, b, $c \in \mathbb{Z}$, and let $g = 1 - f^{p-1}$. Show that for any x, y, $z \in \mathbb{Z}$, $g(x,y,z) \equiv 0$ or $1 \pmod{p}$, and that

$$\sum_{x,y,z \in \{0,1,\ldots,p-1\}} g(x,y,z) \equiv 0 \pmod{p}.$$

Hence show that there exist integers x, y, z, not all divisible by p, such that $f(x,y,z) \equiv 0 \pmod{p}$.

Paper 1, Section I

1G Number Theory

(a) State and prove the Chinese remainder theorem.

(b) An integer n is *squarefull* if whenever p is prime and $p|n$, then $p^2|n$. Show that there exist 1000 consecutive positive integers, none of which are squarefull.

Paper 2, Section I

1G Number Theory

Define the *Legendre symbol*, and state Gauss's lemma. Show that if p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Use the law of quadratic reciprocity to compute $\left(\dfrac{105}{149}\right)$.

Paper 3, Section I

1G Number Theory

What is a *multiplicative function*? Show that if $f(n)$ is a multiplicative function, then so is $g(n) = \sum_{d|n} f(d)$.

Define the *Möbius function* $\mu(n)$, and show that it is multiplicative. Deduce that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

and that

$$f(n) = \sum_{e|n} \mu(e) g\left(\frac{n}{e}\right).$$

What is $g(n)$ if $f(n) = n$? What is $f(n)$ if $g(n) = n$?

Paper 4, Section I

1G Number Theory

Show that if a continued fraction is periodic, then it represents a quadratic irrational. What number is represented by the continued fraction $[7, 7, 7, \dots]$?

Compute the continued fraction expansion of $\sqrt{23}$. Hence or otherwise find a solution in positive integers to the equation $x^2 - 23y^2 = 1$.

Paper 4, Section II

11G Number Theory

(a) State and prove the Fermat–Euler theorem. Let p be a prime and k a positive integer. Show that $b^k \equiv b \pmod{p}$ holds for every integer b if and only if $k \equiv 1 \pmod{p-1}$.

(b) Let $N \geqslant 3$ be an odd integer and b be an integer with $(b, N) = 1$. What does it mean to say that N is a *Fermat pseudoprime to base* b? What does it mean to say that N is a *Carmichael number*?

Show that every Carmichael number is squarefree, and that if N is squarefree, then N is a Carmichael number if and only if $N \equiv 1 \pmod{p-1}$ for every prime divisor p of N. Deduce that a Carmichael number is a product of at least three primes.

(c) Let r be a fixed odd prime. Show that there are only finitely many pairs of primes p, q for which $N = pqr$ is a Carmichael number.

[*You may assume throughout that* $(\mathbb{Z}/p^n\mathbb{Z})^*$ *is cyclic for every odd prime* p *and every integer* $n \geqslant 1$.]

Paper 3, Section II

11G Number Theory

What does it mean to say that a positive definite binary quadratic form is *reduced*? What does it mean to say that two binary quadratic forms are *equivalent*? Show that every positive definite binary quadratic form is equivalent to some reduced form.

Show that the reduced positive definite binary quadratic forms of discriminant -35 are $f_1 = x^2+xy+9y^2$ and $f_2 = 3x^2+xy+3y^2$. Show also that a prime $p > 7$ is represented by f_i if and only if

$$\left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = \begin{cases} +1 & (i = 1) \\ -1 & (i = 2). \end{cases}$$

Paper 3, Section I

1G Number Theory

Explain what is meant by an *Euler pseudoprime* and a *strong pseudoprime*. Show that 65 is an Euler pseudoprime to the base b if and only if $b^2 \equiv \pm 1 \pmod{65}$. How many such bases are there? Show that the bases for which 65 is a strong pseudoprime do *not* form a subgroup of $(\mathbb{Z}/65\mathbb{Z})^\times$.

Paper 1, Section I

1G Number Theory

Define the *Legendre symbol* $\left(\dfrac{a}{p}\right)$.

State Gauss' lemma and use it to compute $\left(\dfrac{2}{p}\right)$ where p is an odd prime.

Show that if $m \geqslant 4$ is a power of 2, and p is a prime dividing $2^m + 1$, then $p \equiv 1 \pmod{4m}$.

Paper 4, Section I

1G Number Theory

Show that, for $x \geqslant 2$ a real number,

$$\prod_{\substack{p \leqslant x, \\ p \text{ is prime}}} \left(1 - \frac{1}{p}\right)^{-1} > \log x\,.$$

Hence prove that

$$\sum_{\substack{p \leqslant x, \\ p \text{ is prime}}} \frac{1}{p} > \log\log x + c\,,$$

where c is a constant you should make explicit.

Paper 2, Section I

1G Number Theory

State and prove Legendre's formula for $\pi(x)$. Use it to compute $\pi(42)$.

Paper 3, Section II

10G Number Theory

Let d be a positive integer which is not a square. Assume that the continued fraction expansion of $\sqrt{d}$ takes the form $[a_0, \overline{a_1, a_2, \ldots, a_m}]$.

(a) Define the *convergents* p_n/q_n, and show that p_n and q_n are coprime.

(b) The complete quotients θ_n may be written in the form $(\sqrt{d} + r_n)/s_n$, where r_n and s_n are rational numbers. Use the relation

$$\sqrt{d} = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}}$$

to find formulae for r_n and s_n in terms of the p's and q's. Deduce that r_n and s_n are integers.

(c) Prove that Pell's equation $x^2 - dy^2 = 1$ has infinitely many solutions in integers x and y.

(d) Find integers x and y satisfying $x^2 - 67y^2 = -2$.

Paper 4, Section II

10G Number Theory

(a) State Dirichlet's theorem on primes in arithmetic progression.

(b) Let d be the discriminant of a binary quadratic form, and let p be an odd prime. Show that p is represented by some binary quadratic form of discriminant d if and only if $x^2 \equiv d \pmod{p}$ is soluble.

(c) Let $f(x, y) = x^2 + 15y^2$ and $g(x, y) = 3x^2 + 5y^2$. Show that f and g each represent infinitely many primes. Are there any primes represented by both f and g?

Paper 3, Section I

1I Number Theory

Show that the exact power of a prime p dividing $N!$ is $\sum_{j=1}^{\infty} \lfloor \frac{N}{p^j} \rfloor$. By considering the prime factorisation of $\binom{2n}{n}$, show that

$$\frac{4^n}{2n+1} \leqslant \binom{2n}{n} \leqslant (2n)^{\pi(2n)}.$$

Setting $n = \lfloor \frac{x}{2} \rfloor$, deduce that for x sufficiently large

$$\pi(x) > \frac{\lfloor \frac{x}{2} \rfloor \log 3}{\log x} > \frac{x}{2 \log x}.$$

Paper 4, Section I

1I Number Theory

Compute the continued fraction expansion of $\sqrt{14}$, and use it to find two solutions to $x^2 - 14y^2 = 2$ where x and y are positive integers.

Paper 2, Section I

1I Number Theory

Define the *Legendre symbol* and the *Jacobi symbol.* Compute the Jacobi symbols $\left(\frac{202}{11189}\right)$ and $\left(\frac{974}{1001}\right)$, stating clearly any properties of these symbols that you use.

Paper 1, Section I

1I Number Theory

Define the Riemann zeta function $\zeta(s)$ for $\mathrm{Re}(s) > 1$. State and prove the alternative formula for $\zeta(s)$ as an Euler product. Hence or otherwise show that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$.

Paper 4, Section II

10I Number Theory

(a) Define *Euler's totient function* $\phi(n)$ and show that $\sum_{d|n} \phi(d) = n$.

(b) State Lagrange's theorem concerning roots of polynomials mod p.

(c) Let p be a prime. Proving any results you need about primitive roots, show that $x^m \equiv 1 \pmod{p}$ has exactly $(m, p-1)$ roots.

(d) Show that if p and $3p-2$ are both primes then $N = p(3p-2)$ is a Fermat pseudoprime for precisely a third of all bases.

Paper 3, Section II

10I Number Theory

What does it mean for a positive definite binary quadratic form to be *reduced*?

Prove that every positive definite binary quadratic form is equivalent to a reduced form, and that there are only finitely many reduced forms with given discriminant.

State a criterion for a positive integer n to be represented by a positive definite binary quadratic form with discriminant $d < 0$, and hence determine which primes p are represented by $x^2 + xy + 7y^2$.

Paper 4, Section I

1H Number Theory

Show that if $10^n + 1$ is prime then n must be a power of 2. Now assuming n is a power of 2, show that if p is a prime factor of $10^n + 1$ then $p \equiv 1 \pmod{2n}$.

Explain the method of Fermat factorization, and use it to factor $10^4 + 1$.

Paper 3, Section I

1H Number Theory

What does it mean to say that a positive definite binary quadratic form is *reduced*? Find the three smallest positive integers properly represented by each of the forms $f(x, y) = 3x^2 + 8xy + 9y^2$ and $g(x, y) = 15x^2 + 34xy + 20y^2$. Show that every odd integer represented by some positive definite binary quadratic form with discriminant -44 is represented by at least one of the forms f and g.

Paper 2, Section I

1H Number Theory

Define the Euler totient function ϕ and the Möbius function μ. Suppose f and g are functions defined on the natural numbers satisfying $f(n) = \sum_{d|n} g(d)$. State and prove a formula for g in terms of f. Find a relationship between μ and ϕ.

Define the Riemann zeta function $\zeta(s)$. Find a Dirichlet series for $\zeta(s-1)/\zeta(s)$ valid for $\mathrm{Re}(s) > 2$.

Paper 1, Section I

1H Number Theory

Define the Legendre symbol $\left(\frac{a}{p}\right)$. State and prove Euler's criterion, assuming if you wish the existence of primitive roots mod p.

By considering the prime factors of $n^2 + 4$ for n an odd integer, prove that there are infinitely many primes p with $p \equiv 5 \pmod 8$.

Paper 4, Section II
9H Number Theory

State the Chinese Remainder Theorem.

Let N be an odd positive integer. Define the Jacobi symbol $\left(\frac{a}{N}\right)$. Which of the following statements are true, and which are false? Give a proof or counterexample as appropriate.

(i) If $\left(\frac{a}{N}\right) = 1$ then the congruence $x^2 \equiv a \pmod{N}$ is soluble.

(ii) If N is not a square then $\sum_{a=1}^{N} \left(\frac{a}{N}\right) = 0$.

(iii) If N is composite then there exists an integer a coprime to N with

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

(iv) If N is composite then there exists an integer a coprime to N with

$$a^{(N-1)/2} \not\equiv \left(\frac{a}{N}\right) \pmod{N}.$$

Paper 3, Section II
9H Number Theory

Let θ be a real number with continued fraction expansion $[a_0, a_1, a_2, \ldots]$. Define the convergents p_n/q_n (by means of recurrence relations) and show that for $\beta > 0$ we have

$$[a_0, a_1, \ldots, a_{n-1}, \beta] = \frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-1} + q_{n-2}}.$$

Show that

$$\left| \theta - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}$$

and deduce that $p_n/q_n \to \theta$ as $n \to \infty$.

By computing a suitable continued fraction expansion, find solutions in positive integers x and y to each of the equations $x^2 - 53y^2 = 4$ and $x^2 - 53y^2 = -7$.

Paper 4, Section I

1F Number Theory

State the Chinese Remainder Theorem.

Find all solutions to the simultaneous congruences

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7). \end{aligned}$$

A positive integer is said to be *square-free* if it is the product of distinct primes. Show that there are 100 consecutive numbers that are not square-free.

Paper 3, Section I

1F Number Theory

Show that the continued fraction for $\sqrt{51}$ is $[7; \overline{7, 14}]$.

Hence, or otherwise, find positive integers x and y that satisfy the equation $x^2 - 51y^2 = 1$.

Are there integers x and y such that $x^2 - 51y^2 = -1$?

Paper 2, Section I

1F Number Theory

Show that

$$\sum_{p \leqslant x} \frac{1}{p} \geqslant \log\log x - \frac{1}{2}.$$

Deduce that there are infinitely many primes.

Paper 1, Section I

1F Number Theory

Define what it means for a number N to be a *pseudoprime* to the base b.

Show that if there is a base b to which N is not a pseudoprime, then N is a pseudoprime to at most half of all possible bases.

Let n be an integer greater than 1 such that $F_n = 2^{2^n} + 1$ is composite. Show that F_n is a pseudoprime to the base 2.

Paper 4, Section II

11F Number Theory

Define the *Legendre* and *Jacobi symbols.*

State the law of quadratic reciprocity for the Legendre symbol.

State the law of quadratic reciprocity for the Jacobi symbol, and deduce it from the corresponding result for the Legendre symbol.

Let p be a prime with $p \equiv 1 \pmod 4$. Prove that the sum of the quadratic residues in the set $\{1, 2, \ldots, p-1\}$ is equal to the sum of the quadratic non-residues in this set.

For which primes p is 7 a quadratic residue?

Paper 3, Section II

11F Number Theory

State and prove Lagrange's theorem about polynomial congruences modulo a prime.

Define the *Euler totient function* ϕ.

Let p be a prime and let d be a positive divisor of $p-1$. Show that there are exactly $\phi(d)$ elements of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ with order d.

Deduce that $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is cyclic.

Let g be a primitive root modulo p^2. Show that g must be a primitive root modulo p.

Let g be a primitive root modulo p. Must it be a primitive root modulo p^2? Give a proof or a counterexample.

Paper 1, Section I

1I Number Theory

State and prove Gauss's Lemma for the Legendre symbol $\left(\frac{a}{p}\right)$. For which odd primes p is 2 a quadratic residue modulo p? Justify your answer.

Paper 4, Section I

1I Number Theory

Let $s = \sigma + it$ with $\sigma, t \in \mathbb{R}$. Define the Riemann zeta function $\zeta(s)$ for $\sigma > 1$. Show that for $\sigma > 1$,

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1},$$

where the product is taken over all primes. Deduce that there are infinitely many primes.

Paper 3, Section I

1I Number Theory

State the Chinese Remainder Theorem.

A composite number n is defined to be a Carmichael number if $b^{n-1} \equiv 1 \mod n$ whenever $(b, n) = 1$. Show that a composite n is Carmichael if and only if n is square-free and $(p-1)$ divides $(n-1)$ for all prime factors p of n. [You may assume that, for p an odd prime and $\alpha \geqslant 1$ an integer, $\left(\mathbb{Z}/p^{\alpha}\mathbb{Z}\right)^{\times}$ is a cyclic group.]

Show that if $n = (6t+1)(12t+1)(18t+1)$ with all three factors prime, then n is Carmichael.

Paper 2, Section I

1I Number Theory

Define Euler's totient function $\phi(n)$, and show that $\sum_{d|n} \phi(d) = n$. Hence or otherwise prove that for any prime p the multiplicative group $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ is cyclic.

Paper 4, Section II

11I Number Theory

(i) What is meant by the continued fraction expansion of a real number θ? Suppose that θ has continued fraction $[a_0, a_1, a_2, \dots]$. Define the convergents p_n/q_n to θ and give the recurrence relations satisfied by the p_n and q_n. Show that the convergents p_n/q_n do indeed converge to θ.

[You need not justify the basic order properties of finite continued fractions.]

(ii) Find two solutions in strictly positive integers to each of the equations

$$x^2 - 10y^2 = 1 \qquad \text{and} \qquad x^2 - 11y^2 = 1\,.$$

Paper 3, Section II

11I Number Theory

Define equivalence of binary quadratic forms and show that equivalent forms have the same discriminant.

Show that an integer n is properly represented by a binary quadratic form of discriminant d if and only if $x^2 \equiv d \mod 4n$ is soluble in integers. Which primes are represented by a form of discriminant -20?

What does it mean for a positive definite form to be reduced? Find all reduced forms of discriminant -20. For each member of your list find the primes less than 100 represented by the form.

Paper 4, Section I

1I Number Theory

Define what it means for the composite natural number N to be a *pseudoprime* to the base b.

Find the number of bases (less than 21) to which 21 is a pseudoprime. [You may, if you wish, assume the Chinese Remainder Theorem.]

Paper 3, Section I

1I Number Theory

Define the *discriminant* of the binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$.

Assuming that this form is positive definite, define what it means for f to be *reduced*.

Show that there are precisely two reduced positive definite binary quadratic forms of discriminant -35.

Paper 2, Section I

1I Number Theory

Define the *Legendre symbol* and the *Jacobi symbol*.

State the law of quadratic reciprocity for the Jacobi symbol.

Compute the value of the Jacobi symbol $\left(\dfrac{247}{321}\right)$, stating clearly any results you use.

Paper 1, Section I

1I Number Theory

Show that the continued fraction for $\sqrt{13}$ is $[3;\overline{1,1,1,1,6}]$.

Hence, or otherwise, find a solution to the equation $x^2 - 13y^2 = 1$ in positive integers x and y. Write down an expression for another solution.

Paper 4, Section II

11I Number Theory

Let $f : \mathbb{N} \to \mathbb{R}$ be a function, where $\mathbb{N}$ denotes the (positive) natural numbers.

Define what it means for f to be a *multiplicative function*.

Prove that if f is a multiplicative function, then the function $g : \mathbb{N} \to \mathbb{R}$ defined by

$$g(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Define the Möbius function μ. Is μ multiplicative? Briefly justify your answer.

Compute

$$\sum_{d|n} \mu(d)$$

for all positive integers n.

Define the Riemann zeta function ζ for complex numbers s with $\Re(s) > 1$.

Prove that if s is a complex number with $\Re(s) > 1$, then

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Paper 3, Section II

11I Number Theory

Let p be an odd prime. Prove that the multiplicative groups $(\mathbb{Z}/p^n\mathbb{Z})^\times$ are cyclic for $n \geqslant 2$. [You may assume that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.]

Find an integer which generates $(\mathbb{Z}/7^n\mathbb{Z})^\times$ for all $n \geqslant 1$, justifying your answer.

Paper 1, Section I
1I Number Theory

Prove that, under the action of $\mathrm{SL}_2(\mathbb{Z})$, every positive definite binary quadratic form of discriminant -163, with integer coefficients, is equivalent to

$$x^2 + xy + 41y^2 \,.$$

Paper 2, Section I
1I Number Theory

(i) Find a primitive root modulo 17.

(ii) Let p be a prime of the form $2^m + 1$ for some integer $m \geqslant 1$. Prove that every quadratic non-residue modulo p is a primitive root modulo p.

Paper 3, Section I
1I Number Theory

(i) State Lagrange's Theorem, and prove that, if p is an odd prime,

$$(p-1)! \equiv -1 \mod p \,.$$

(ii) Still assuming p is an odd prime, prove that

$$3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p \,.$$

Paper 4, Section I
1I Number Theory

(i) Prove that there are infinitely many primes.

(ii) Prove that arbitrarily large gaps can occur between consecutive primes.

Paper 3, Section II

11I Number Theory

Let $\zeta(s)$ be the Riemann zeta function, and put $s = \sigma + it$ with $\sigma, t \in \mathbb{R}$.

(i) If $\sigma > 1$, prove that

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}\,,$$

where the product is taken over all primes p.

(ii) Assuming that, for $\sigma > 1$, we have

$$\zeta(s) = \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s})\,,$$

prove that $\zeta(s) - \frac{1}{s-1}$ has an analytic continuation to the half plane $\sigma > 0$.

Paper 4, Section II

11I Number Theory

(i) Prove the law of reciprocity for the Jacobi symbol. You may assume the law of reciprocity for the Legendre symbol.

(ii) Let n be an odd positive integer which is not a square. Prove that there exists an odd prime p with $\left(\frac{n}{p}\right) = -1$.

Paper 1, Section I

1G Number Theory

(i) Let N be an integer $\geqslant 2$. Define the addition and multiplication on the set of congruence classes modulo N.

(ii) Let an integer $M \geqslant 1$ have expansion to the base 10 given by $a_s \ldots a_0$. Prove that 11 divides M if and only if $\sum_{i=0}^{s} (-1)^i a_i$ is divisible by 11.

Paper 2, Section I

1G Number Theory

Let p be an odd prime number. If n is an integer prime to p, define $\left(\frac{n}{p}\right)$.

(i) Prove that $\chi(n) = \left(\frac{n}{p}\right)$ defines a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^{\times}$ to the group $\{\pm 1\}$. What is the value of $\chi(-1)$?

(ii) If $p \equiv 1 \bmod 4$, prove that $\sum_{n=1}^{p-1} \chi(n)\, n = 0$.

Paper 3, Section I

1G Number Theory

(i) Let M and N be positive integers, such that N is not a perfect square. If $M < \sqrt{N}$, show that every solution of the equation

$$x^2 - Ny^2 = M$$

in positive integers x, y comes from some convergent of the continued fraction of $\sqrt{N}$.

(ii) Find a solution in positive integers x, y of

$$x^2 - 29y^2 = 5 .$$

Paper 4, Section I

1G Number Theory

Let p be a prime number, and put

$$a_k = kp\,, \quad N_k = a_k^p - 1 \quad (k = 1, 2, \dots)\,.$$

Prove that a_k has exact order p modulo N_k for all $k \geqslant 1$, and deduce that N_k must be divisible by a prime q with $q \equiv 1 \pmod{p}$. By making a suitable choice of k, prove that there are infinitely many primes q with $q \equiv 1 \pmod{p}$.

Paper 3, Section II

11G Number Theory

State precisely the Miller-Rabin primality test.

(i) Let p be a prime $\geqslant 5$, and define

$$N = \frac{4^p - 1}{3}\,.$$

Prove that N is a composite odd integer, and that N is a pseudo-prime to the base 2.

(ii) Let M be an odd integer greater than 1 such that M is a pseudo-prime to the base 2. Prove that $2^M - 1$ is always a strong pseudo-prime to the base 2.

Paper 4, Section II

11G Number Theory

Let $\mathcal{S}$ be the set of all positive definite binary quadratic forms with integer coefficients. Define the action of the group $SL_2(\mathbb{Z})$ on $\mathcal{S}$, and prove that equivalent forms under this action have the same discriminant.

Find necessary and sufficient conditions for an odd positive integer n, prime to 35, to be properly represented by at least one of the two forms

$$x^2 + xy + 9y^2\,, \qquad 3x^2 + xy + 3y^2\,.$$

Paper 1, Section I

1G Number Theory

State the Chinese Remainder Theorem.

Determine all integers x satisfying the congruences $x \equiv 2 \bmod 3$, $x \equiv 2 \bmod 5$, $x \equiv 6 \bmod 7$.

Paper 2, Section I

1G Number Theory

State the law of quadratic reciprocity for the Jacobi symbol $\left(\frac{m}{n}\right)$, where m, n are odd positive integers, and prove this law using the reciprocity law for the Legendre symbol.

Compute the Jacobi symbol $\left(\frac{261}{317}\right)$.

Paper 3, Section I

1G Number Theory

For any integer $x \geqslant 2$, define $\theta(x) = \sum_{p \leqslant x} \log p$, where the sum is taken over all primes $p \leqslant x$. Put $\theta(1) = 0$. By studying the integer

$$\binom{2n}{n},$$

where $n \geqslant 1$ is an integer, prove that

$$\theta(2n) - \theta(n) < 2n \log 2.$$

Deduce that

$$\theta(x) < (4 \log 2)x,$$

for all $x \geqslant 1$.

Paper 4, Section I

1G Number Theory

Let W denote the set of all positive definite binary quadratic forms, with integer coefficients, and having discriminant -67. Let $SL_2(\mathbb{Z})$ be the group of all 2×2 matrices with integer entries and determinant 1. Prove that W is infinite, but that all elements of W are equivalent under the action of the group $SL_2(\mathbb{Z})$

Paper 3, Section II

11G Number Theory

Let p be an odd prime. Prove that there is an equal number of quadratic residues and non-residues in the set $\{1, \ldots, p-1\}$.

If n is an integer prime to p, let m_n be an integer such that $nm_n \equiv 1 \bmod p$. Prove that

$$n(n+1) \equiv n^2(1+m_n) \bmod p,$$

and deduce that

$$\sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p} \right) = -1.$$

Paper 4, Section II

11G Number Theory

Let $s = \sigma + it$, where σ and t are real, and for $\sigma > 1$ let

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,.$$

Prove that $\zeta(s)$ has no zeros in the half plane $\sigma > 1$. Show also that for $\sigma > 1$,

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\,,$$

where μ denotes the Möbius function. Assuming that $\zeta(s) - \dfrac{1}{s-1}$ has an analytic continuation to the half plane $\sigma > 0$, show that if $s = 1 + it$, with $t \neq 0$, and $\zeta(s) = 0$ then s is at most a simple zero of ζ.

1/I/1H **Number Theory**

Define the continued fraction of a real number α.

Compute the continued fraction of $\sqrt{19}$.

2/I/1H **Number Theory**

What does it mean for a positive definite quadratic form with integer coefficients to be reduced?

Show that there are precisely three reduced forms of this type with discriminant equal to -23.

Which odd primes are properly represented by some positive definite binary quadratic form (with integer coefficients) of discriminant -23?

3/I/1H **Number Theory**

Prove that, for all $x \geqslant 2$, we have

$$\sum_{p \leqslant x} \frac{1}{p} > \log\log x - \frac{1}{2}.$$

[You may assume that, for $0 < u < 1$,

$$-\log(1-u) - u < \frac{u^2}{2(1-u)}.]$$

3/II/11H **Number Theory**

State the reciprocity law for the Jacobi symbol.

Let a be an odd integer > 1, which is not a square. Prove that there exists a positive integer n such that $n \equiv 1 \bmod 4$ and

$$\left(\frac{n}{a}\right) = -1.$$

Prove further that there exist infinitely many prime numbers p such that

$$\left(\frac{a}{p}\right) = -1.$$

4/I/1H **Number Theory**

Let p be an odd prime number. Assuming that the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is cyclic, prove that the multiplicative group of units of $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic for all $n \geqslant 1$.

Find an integer a such that its residue class in $\mathbb{Z}/11^n\mathbb{Z}$ generates the multiplicative group of units for all $n \geqslant 1$.

4/II/11H **Number Theory**

Let $N > 1$ be an integer, which is not a square, and let p_k/q_k ($k = 1, 2, \ldots$) be the convergents to $\sqrt{N}$. Prove that

$$|p_k^2 - q_k^2 N| < 2\sqrt{N} \quad (k = 1, 2, \ldots).$$

Explain briefly how this result can be used to generate a factor base B, and a set of B-numbers which may lead to a factorization of N.

1/I/1F **Number Theory**

State the prime number theorem, and Bertrand's postulate.

Let S be a finite set of prime numbers, and write $f_s(x)$ for the number of positive integers no larger than x, all of whose prime factors belong to S. Prove that

$$f_s(x) \leqslant 2^{\#(S)}\sqrt{x},$$

where $\#(S)$ denotes the number of elements in S. Deduce that, if x is a strictly positive integer, we have

$$\pi(x) \geqslant \frac{\log x}{2\log 2}.$$

2/I/1F **Number Theory**

Let p be an odd prime number. Prove that 2 is a quadratic residue modulo p when $p \equiv 7 \pmod 8$. Deduce that, if q is a prime number strictly greater than 3 with $q \equiv 3 \pmod 4$ such that $2q+1$ is also a prime number, then $2^q - 1$ is necessarily composite. Why does the argument break down for $q = 3$?

3/I/1F **Number Theory**

Determine the continued fraction of $\sqrt{7}$. Deduce two pairs of solutions in positive integers x, y of the equation

$$x^2 - 7y^2 = 1.$$

3/II/11F **Number Theory**

State the Chinese remainder theorem. Let n be an odd positive integer. If n is divisible by the square of a prime number p, prove that there exists an integer z such that $z^p \equiv 1 \pmod{n}$ but $z \not\equiv 1 \pmod{n}$.

Define the Jacobi symbol

$$\left(\frac{a}{n}\right)$$

for any non-zero integer a. Give a numerical example to show that

$$\left(\frac{a}{n}\right) = +1$$

does not imply in general that a is a square modulo n. State and prove the law of quadratic reciprocity for the Jacobi symbol.

[*You may assume the law of quadratic reciprocity for the Legendre symbol.*]

Assume now that n is divisible by the square of a prime number. Prove that there exists an integer a with $(a, n) = 1$ such that the congruence

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

does not hold. Show further that this congruence fails to hold for at least half of all relatively prime residue classes modulo n.

4/I/1F **Number Theory**

Prove Legendre's formula relating $\pi(x)$ and $\pi(\sqrt{x})$ for any positive real number x. Use this formula to compute $\pi(48)$.

4/II/11F **Number Theory**

Let p be a prime number, and let $f(x)$ be a polynomial with integer coefficients, whose leading coefficient is not divisible by p. Prove that the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most d solutions, where d is the degree of $f(x)$.

Deduce that all coefficients of the polynomial

$$x^{p-1} - 1 - \big((x-1)(x-2)\cdots(x-p+1)\big)$$

must be divisible by p, and prove that:

(i) $(p-1)! + 1 \equiv 0 \pmod{p}$;

(ii) if p is odd, the numerator of the fraction

$$u_p = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

is divisible by p.

Assume now that $p \geqslant 5$. Show by example that (i) cannot be strengthened to $(p-1)! + 1 \equiv 0 \pmod{p^2}$.

1/I/1H Number Theory

State the theorem of the primitive root for an odd prime power modulus.

Prove that 3 is a primitive root modulo 7^n for all integers $n \geqslant 1$. Is 2 a primitive root modulo 7^n for all integers $n \geqslant 1$?

Prove that there is no primitive root modulo 8.

2/I/1H Number Theory

Prove that all binary quadratic forms of discriminant -7 are equivalent to $x^2 + xy + 2y^2$.

Determine which prime numbers p are represented by $x^2 + xy + 2y^2$.

3/I/1H Number Theory

Let $N = p_1 p_2 \dots p_r$ be a product of distinct primes, and let $\lambda(N)$ be the least common multiple of $p_1 - 1, p_2 - 1, \dots, p_r - 1$. Prove that

$$a^{\lambda(N)} \equiv 1 \bmod N \quad \text{when} \quad (a, N) = 1.$$

Now take $N = 7 \times 13 \times 19$, and prove that

$$a^{N-1} \equiv 1 \bmod N \quad \text{when} \quad (a, N) = 1.$$

3/II/11H Number Theory

State the prime number theorem, and Dirichlet's theorem on primes in arithmetic progression.

If p is an odd prime number, prove that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \mod 4$.

Let $p_1, \dots, p_m$ be distinct prime numbers, and define

$$N_1 = 4p_1 \dots p_m - 1, \quad N_2 = 4\left(p_1 \dots p_m\right)^2 + 1.$$

Prove that N_1 has at least one prime factor which is congruent to 3 mod 4, and that every prime factor of N_2 must be congruent to 1 mod 4.

Deduce that there are infinitely many primes which are congruent to 1 mod 4, and infinitely many primes which are congruent to 3 mod 4.

4/I/1H **Number Theory**

Let x be a real number greater than or equal to 2, and define

$$P(x) = \prod_{p \leqslant x} \left(1 - \frac{1}{p}\right),$$

where the product is taken over all primes p which are less than or equal to x. Prove that $P(x) \to 0$ as $x \to \infty$, and deduce that $\sum_p \frac{1}{p}$ diverges when the summation is taken over all primes p.

4/II/11H **Number Theory**

Define the notion of a Fermat, Euler, and strong pseudo-prime to the base b, where b is an integer greater than 1.

Let N be an odd integer greater than 1. Prove that:

(a) If N is a prime number, then N is a strong pseudo-prime for every base b with $(b, N) = 1$.

(b) If there exists a base b_1 with $1 < b_1 < N$ and $(b_1, N) = 1$ for which N is not a pseudo-prime, then in fact N is not a pseudo-prime for at least half of all bases b with $1 < b < N$ and $(b, N) = 1$.

Prove that 341 is a Fermat pseudo-prime, but not an Euler pseudo-prime, to the base 2.

1/I/1H **Number Theory**

Define the Legendre symbol $\left(\frac{a}{p}\right)$. Prove that, if p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Use the law of quadratic reciprocity to calculate $\left(\frac{91}{167}\right)$.

[*You may use the Gauss Lemma without proof.*]

2/I/1H **Number Theory**

Recall that, if p is an odd prime, a *primitive root* modulo p is a generator of the cyclic (multiplicative) group $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Let p be an odd prime of the form $2^{2^n}+1$; show that a is a primitive root mod p if and only if a is not a quadratic residue mod p. Use this result to prove that 7 is a primitive root modulo every such prime.

3/I/1H **Number Theory**

Let $\pi(x)$ be the number of primes $p \leqslant x$. State the Legendre formula, and prove that

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0.$$

[*You may use the formula*

$$\prod_{p\leqslant x} (1-1/p)^{-1} \geqslant \log x$$

without proof.]

3/II/11H **Number Theory**

Show that there are exactly two reduced positive definite integer binary quadratic forms with discriminant -20; write these forms down.

State a criterion for an odd integer n to be properly represented by a positive definite integer binary quadratic form of given discriminant d.

Describe, in terms of congruences modulo 20, which primes other than $2, 5$ are properly represented by the form x^2+5y^2, and justify your answer.

4/I/1H Number Theory

If n is an odd integer and b is an integer prime with n, state what it means for n to be a pseudoprime to the base b. What is a Carmichael number? State a criterion for n to be a Carmichael number and use the criterion to show that:

(i) Every Carmichael number is the product of at least three distinct primes.

(ii) 561 is a Carmichael number.

4/II/11H Number Theory

(a) Let N be a non-square integer. Describe the integer solutions of the Pell equation $x^2 - Ny^2 = 1$ in terms of the convergents to $\sqrt{N}$. Show that the set of integer solutions forms an abelian group. Denote the addition law in this group by $\circ$; given solutions (x_0, y_0) and (x_1, y_1), write down an explicit formula for $(x_0, y_0) \circ (x_1, y_1)$. If (x, y) is a solution, write down an explicit formula for $(x, y) \circ (x, y) \circ (x, y)$ in the group law.

(b) Find the continued fraction expansion of $\sqrt{11}$. Find the smallest solution in integers $x, y > 0$ of the Pell equation $x^2 - 11y^2 = 1$. Use the formula in Part (a) to compute $(x, y) \circ (x, y) \circ (x, y)$.