PartII Number Theory

zc231

Each question will be labeled in the form $\alpha, \beta\gamma$ where $\alpha \in \{1, 2, 3, 4\}$ represents the paper number, $\beta\gamma$ represents the question number in that paper. For example, 1,11G means question 11G in paper 1. I will omit the proofs in the notes or book work. The solutions provided might not be the best ways to solve the problems and if you find any mistakes or if you have any elegant ways of solving some of the problems please email me at zc231@cam.ac.uk.

2009

1,1G $x \equiv 62 \bmod 105$.

2,1G $\left(\frac{261}{317}\right) = \left(\frac{56}{261}\right) = \left(\frac{2}{261}\right)\left(\frac{7}{261}\right) = (-1)\left(\frac{2}{7}\right) = -1$.

3,1G Note if you take exponential of $\theta(x)$ then it is the product of all prime numbers less than or equal to x. Thus,

$$\frac{e^{\theta(2n)}}{e^{\theta(n)}} = \prod_{n<p\leq 2n} p \leq \binom{2n}{n}$$

because $\binom{2n}{n}$ is an integer and each p with $n < p \leq 2n$ divides this quantity. Finally, $\binom{2n}{n}$ is one of the term in the binomial expansion of $2^n = (1+1)^{2n}$ therefore

$$\frac{e^{\theta(2n)}}{e^{\theta(n)}} \leq \binom{2n}{n} < 2^{2n}$$

and taking logarithm gives the first part.

It is clear that $\theta(x)$ is an increasing function. For all $x \geq 1$ pick n with $2^{n-1} \leq x < 2^n$. Now

$$\theta(2^n) - \theta(2^{n-1}) < 2^n \log 2, \theta(2^{n-1}) - \theta(2^{n-2}) < 2^{n-1}\log 2, \cdots, \theta(2) - \theta(1) < 2\log 2$$

so if you sum over these inequalities and use the convention $\theta(1) = 0$ you then have $\theta(2^n) < 2(2^n - 1)\log 2 < 2^{n+1}\log 2$. Therefore,

$$\theta(x) < \theta(2^n) < 2^{n+1}\log 2 = (4\log 2)2^{n-1} \leq (4\log 2)x$$

by our choice of n.

4,1G Any binary form with discriminant -67 has the property $4ac - b^2 = 67$ and let $b = 2k+1$ be an odd number then this reduces to $ac - k^2 - k = 17$. Thus for each k, let $a = 1$, $b = 2k+1$ and $c = 17 + k^2 + 17$ we have a binary form with discriminant -67 and hence there exists infinitely many of them. Then one checks the only reduced binary form with discriminant -67 is $x^2 + xy + 17y^2$.

3,11G The first part is book work. It is clear by definition of m_n that the congruence relation holds (if you expand the bracket on RHS). Then finally,

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

Therefore,

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

because there is a bijection between the sets $\{m_n : n = 1, \dots, p-1\}$ and $\{n : n = 1, \dots, p-1\}$ (as inverse exists and is unique). Finally, let $m = n + 1$

$$\sum_{n=1}^{p-1}\left(\frac{1+n}{p}\right) = \sum_{m=2}^{p}\left(\frac{m}{p}\right) = \sum_{m=1}^{p-1}\left(\frac{m}{p}\right) - \left(\frac{1}{p}\right) = \sum_{m=1}^{p-1}\left(\frac{m}{p}\right) - 1$$

where the first term is 0 because the number of residues is the same as the number of non-residues so the result is just -1.

4,11G The first part is book work. For $\sigma > 1$ we can use the Euler product so

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

Use the above equality, by taking modulus and using triangle inequality we have

$$\left|\frac{1}{\zeta(s)}\right| \leq \sum_{n=1}^{\infty} |\mu(n) n^{-s}| = \sum_{n=1}^{\infty} \mu(n) n^{-\sigma} = \zeta(\sigma).$$

Suppose we have a double zero at $1 + it$ for some $t \in \mathbb{R}$, then by the inequality above we must have an double zero at $1 + it$ for $\frac{1}{\zeta(s)}$, which means $\zeta(s)$ has a double pole. But $\zeta(s) - \frac{1}{s-1}$ has an analytic continuation and so $\zeta(s)$ only has a simple pole at $s = 1$, which is a contradiction.

2010

1,1G Addition: $[a]+[b]=[a+b]$. Multiplication $[a][b]=[ab]$ where $[a]$ is the equivalence class containing integers which are congruent to a modulo N.

Observe that $10^i \equiv (-1)^i \bmod 11$. Thus,

$$\sum_{i=0}^{s} 10^i a_i \equiv \sum_{i=0}^{s} (-1)^i a_i \bmod 11$$

and so it is divisible by 11 if and only if RHS is divisible by 11.

2,1G $\left(\frac{n}{p}\right)=0$ if p divides n and for $p \nmid n$, $\left(\frac{n}{p}\right)=1$ if n is a square mod p and -1 if n is not a square mod p.

The first part is book work (use Euler's criteria). $\chi(-1)=(-1)^{\frac{p-1}{2}}$. If $p \equiv 1 \bmod 4$ then $\chi(n)=\chi(p-n)$. Also the set $\{n : n=1,\dots,p-1\}$ is bijective to $\{p-n : n=1,\dots,p-1\}$ so

$$\sum_{n=1}^{p-1} \chi(n)n = \sum_{n=1}^{p-1} \chi(p-n)(p-n) = \sum_{n=1}^{p-1} \chi(n)(p-n).$$

Therefore,

$$2\sum_{n=1}^{p-1} \chi(n)n = \sum_{n=1}^{p-1} \chi(n)n + \sum_{n=1}^{p-1} \chi(n)(p-n) = p\sum_{n=1}^{p-1} \chi(n) = 0.$$

3,1G The first part is question 1 in example sheet 4. $x=11, y=2$.

4,1G $a_k^p \equiv 1 \bmod N_k$ and p is the smallest power of a_k which is bigger than N_k so it is the order. Let $N_k = q_1^{e_1}\cdots q_n^{e_n}$ where q_i are distinct primes and $e_i \geq 1$. By Euler we have

$$a_k^{\phi(N_k)} \equiv 1 \bmod N_k$$

and thus p divides $\phi(N_k)=\prod_{i=1}^{n}(q_i-1)\prod_{i=1}^{n} q_i^{e_i-1}$. But as p divides a_k and a_k is coprime to N_k so p does not divide any q_i thus p divides some q_i-1 for some i and so $q_i \equiv 1 \bmod p$.

Suppose there are only finitely many such q, say $q_1,\dots,q_r$. Let $a_k = kp$ with $k = q_1q_2\cdots q_r$. Then by above argument we have some prime factor q of N_k with $q \equiv 1 \bmod p$. Since k divides a_k and a_k is coprime to N_k so k is coprime to N_k and hence coprime to q. Thus, $q \neq q_i$ for any i which is a contradiction.

3,11G The first part is not in syllabus any more (Miller-Rabin). $3N = 4^p - 1 = (2^p+1)(2^p-1)$ and since $p \geq 5$ so neither factor is trivial or divisible by 3 so N is composite. $N-1=4t$ where $t=\frac{4^{p-1}-1}{3}$. By Fermat's little theorem, p divides $4^{p-1}-1$ and $p \geq 5$ so p divides t and let $t=kp$ where k is odd. Therefore,

$$2^{N-1} \equiv 2^{4kp} \equiv (4^p)^{2k} \equiv 1 \bmod N$$

as $4^p = 1+3N$.

For the second part, write $N=2^M-1$ and so $N-1=2^M-2=2t$ where $t=2^{M-1}-1$ is odd. As M is a pseudo prime to the base 2 we have

$$2^{M-1} \equiv 1 \bmod M$$

and so M divides t so let $t=kM$ where k is odd. Further, $2^M = 1+N$ so $2^M \equiv 1 \bmod N$. Therefore,

$$2^t \equiv (2^M)^k \equiv 1 \bmod N.$$

4,11G The first part is book work. For the second part, firstly check that these two are the only reduced forms with discriminant -35. Then as we assume n is odd and prime to 35, let

$$n = \prod_i p_i^{e_i}, p_i \neq 2, 5, 7.$$

So we work out the congruence condition on these primes p_i. We require

$$-35 \equiv x^2 \bmod 4n$$

to be solvable. Thus, by Chinese remainder theorem, we require -35 to be a square mod 4 and a square mod $p_i^{e_i}$ for each i. As $p_i \neq 2$ so by Hensel's lemma -35 is a square mod $p_i^{e_i}$ if and only if -35 is a square mod p_i. Therefore we need

$$\left(\frac{-35}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{-7}{p}\right) = \left(\frac{p}{5}\right)\left(\frac{p}{7}\right) = 1$$

and so either $p_i \equiv \pm 1 \bmod 5$, $p_i \equiv 1, 2, 4 \bmod 7$ or $p_i \equiv \pm 2 \bmod 5$, $p_i \equiv 3, 5, 6 \bmod 7$.

2011

1,1G Standard.

2,1G 3 is primitive mod 17. Let $p = 2^m + 1$ for each $(a, p) = 1$ we have $a^{p-1} \equiv 1 \bmod p$ and $p - 1 = 2^m$ so if d is the order of a then d divides 2^m so d is a power of 2. Pick a generator g and let $a = g^e$ for some integer e. Then

$$a^d \equiv g^{ed} \equiv g^{2^k e} \equiv 1 \bmod p.$$

Therefore, 2^m divides $2^k e$ and if $k < m$ then e must be a power of 2, hence even. This shows that if a is not primitive (so $k < m$) then $a = g^e$ with e even and so a is a quadratic residue mod p.

3,1G $x^2 \equiv 1 \bmod p$ if and only if $x \equiv \pm 1 \bmod p$ so if we pair each a with its inverse b (with $ab \equiv 1 \bmod p$) the only integers left are $1, p - 1$ therefore,

$$(p - 2)! \equiv 1 \bmod p$$

and so $(p - 1)! \equiv -1 \bmod p$.

For the second part,

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv 1 \cdot (p-2) \cdot 3 \cdot (p-4) \cdots (p-2) \cdot 1 \equiv (p-1)!(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{2}} \bmod p$$

4,1G $n! + 1$ is divisible by some prime bigger than n. For the second part, fix an integer M and then none of the integers in the set $\{M! + n : n = 2, 3, \ldots, M\}$ is prime.

3,11I This question is book work.

4,11I The first part is book work. For the second part, write

$$n = a^2 \prod_i p_i, p_i \text{ distinct odd primes.}$$

Pick m which satisfies the following congruence relations,

$$m \equiv 1 \bmod 4, m \equiv b \bmod p_1, m \equiv 1 \bmod p_i, i \neq 1$$

where $\left(\frac{b}{p_1}\right) = -1$. Then we have

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = \prod_i \left(\frac{m}{p_i}\right) = -1.$$

Therefore, by definition of Jacobi symbol, there must exist a prime factor p of m with $\left(\frac{n}{p}\right) = -1$.

This question only asks for the case n is odd, when n is even, take $m \equiv 1 \bmod 8$ instead of $m \equiv 1 \bmod 4$. If further they ask you to prove there exist infinitely many such p, then suppose there are only finitely many, say $p_1, \ldots, p_r$, add the congruence relation $m \equiv 1 \bmod p_i, i = 1, \ldots, r$ so that the prime factor p cannot be any p_i.

2012

1,1I Standard.

2,1I
$$\left(\frac{321}{247}\right) = \left(\frac{2}{247}\right)\left(\frac{37}{247}\right) = -\left(\frac{25}{37}\right) = -1.$$

3,1I $x^2 + xy + 9y^2$ and $3x^2 + xy + 3y^2$.

4,1I By Chinese remainder theorem we need $b^{20} \equiv 1 \bmod 3, 7$. By Fermat's little theorem, we have $b^2 \equiv 1 \bmod 3$ so $b^{20} \equiv (b^2)^{10} \equiv 1 \bmod 3$. $b^6 \equiv 1 \bmod 7$ so $b^{18} \equiv 1 \bmod 7$ and so $b^{20} \equiv b^2 \bmod 7$. Therefore we need
$$b^2 \equiv 1 \bmod 7$$
which gives $b \equiv \pm 1 \bmod 7$ and so we have 4 solutions less than 21.

3,11I The first part is book work and further by the proof of the first part we know to find generators for $(\mathbb{Z}/7^n\mathbb{Z})^*$ it suffices to find g with $g^6 = 1 + bp, (b, p) = 1$. For example we can pick 2.

4,11I f is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.
$$g(mn) = \sum_{d\left|mn\right.} f(d) = \sum_{d_1\left|m, d_2\right|n} f(d_1 d_2) = \sum_{d_1\left|m\right.} f(d_1) \sum_{d_2\left|n\right.} f(d_2)$$
because $(m, n) = 1$ (so d divides the product of them means $d = d_1 d_2$ with $d_1\left|m, d_2\right|n$).

$\mu(n) = 1$ if $n = 1$, $\mu(n) = 0$ if n is not square free and $\mu(n) = (-1)^k$ where k is the number of distinct prime factor of n if n is square free. It is multiplicative and hence $\sum_{d\left|n\right.} \mu(d)$ is multiplicative. For each $p^k, k \geq 1$, we have
$$\sum_{d\left|p^k\right.} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) = 1 - 1 + 0 + \cdots + 0 = 0.$$
Therefore, if $n \geq 2$, the sum is zero by using multiplicity and the sum is 1 if $n = 1$.

If you want to show the last part without using Euler's product (I guess you have to prove the expansion converges in this question because the first several parts have nothing to do with $\zeta(s)$), then you consider
$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{m,n=1}^{\infty} \frac{\mu(n)}{(mn)^s} = \sum_{d=1}^{\infty} \frac{g(d)}{d^s}$$
where we write $d = mn$ and $g(d) = \sum_{n\left|d\right.} \mu(n)$ which is 1 if $d = 1$ and 0 otherwise. Therefore, the product is just 1. You need the real part of s greater than 1 because then $\zeta(s)$ converges absolutely so in the product above, you can rearrange the order of the sum (recall from 1A analysis).

2013

1,1I book work.

2,1I $\phi(n)$ is the number of positive integers less than n which is coprime to n and for convention $\phi(1) = 1$. $\phi(n)$ is multiplicative and hence $\sum_{d|n} \phi(d)$ is multiplicative. We have for any prime p and $k \geq 1$,

$$\sum_{d|p^k} \phi(d) = \phi(1) + \phi(p) + \cdots + \phi(p^k) = 1 + (p-1) + \cdots + (p^k - p^{k-1}) = p^k.$$

Therefore, by writing $n = \prod_i p_i^{e_i}$ we conclude that $\sum_{d|n} \phi(d) = n$.

Let $n = p - 1$ and let $f(d)$ be the number of elements with exact order d (so $d|n$ by Lagrange theorem). Suppose an element x has order d, then for any a with $(a, d) = 1$, the element x^a also has order d because consider the group generated by x, then there exists b with $ab \equiv 1 \mod d$ so $x \equiv (x^a)^b \mod p$ and so x is a power of x^a so x^a is another generator. This shows x has order d if and only if x^a has order d for all $(a, d) = 1$.

Therefore, if $f(d) > 0$ then $f(d) = \phi(d)$. As we must have

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

we conclude that $f(d) > 0$ for all d and in particular, $f(p-1) > 0$ so there exists an element of order $p - 1$ which generates the group.

3,1I This is question 5 and 6 on sheet 4.

4,1I The first part is book work. As $\zeta(s)$ has a simple pole at $s = 1$ so as $s \to 1$ the quantity $|\zeta(s)|$ should be unbounded, but if there are only finitely many primes the Euler product is a finite product which is bounded.

3,11I We require $x^2 \equiv -20 \mod 4p$ to be solvable. This is clearly true for $p = 2$. Now for $p \neq 2$, by Chinese remainder theorem it reduces to find p with $\left(\frac{-20}{p}\right) = 1$, which is

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right) = 1$$

so we have $p \equiv 1, 3, 7, 9 \mod 20$.

Reduced forms of discriminant -20: $x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$. Note that

$$x^2 + 5y^2 \equiv x^2 \mod 5, 2x^2 + 2xy + 3y^2 \equiv 2(x - 2y)^2 \mod 5$$

therefore combine with what we have from the previous part, if p is represented by $x^2 + 5y^2$, then $p \equiv 1, 9 \mod 20$ and if p is represented by $2x^2 + 2xy + 3y^2$ then $p \equiv 3, 7 \mod 20$. So for $x^2 + 5y^2$ we have $29, 41, 61, 89$ and for $2x^2 + 2xy + 3y^2$ we have $3, 7, 23, 43, 47, 67, 83$.

4,11I This question is basically book work. To prove p_n/q_n converges to θ you only need to prove the inequality

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

and states the fact q_n is strictly increasing (hence unbounded).