EXAMINATION SOLUTIONS
UNIVERSITY OF BRISTOL

Examination for the Degree of B.Sc. and M.Sci. (Level III)

NUMBER THEORY
MATH 30200
(Paper Code MATH-30200)

May-June 2015
[B]=bookwork, [H]=variant of homework problem, [U]=unseen

1. (25 marks total)

(a) (2+4 marks; [B+H]) (i) Quadratic Reciprocity: Let p and q be distinct odd prime numbers. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

(ii) First note that 5 is a quadratic residue modul0 2, since $5 \equiv 1^2 \pmod 2$. If 5 is to be a quadratic residue modulo an odd prime $p \neq 5$, then by quadratic reciprocity,

$$1 = \left(\frac{5}{p}\right) = (-1)^{\frac{1}{4}(5-1)(p-1)}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right).$$

But the quadratic residues modulo 5 are $1^2 \equiv 4^2 \equiv 1 \pmod 5$ and $2^2 \equiv 3^2 \equiv -1 \pmod 5$, and so $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 5$.

(b) (3+2+3 marks; [U resembles H+U+U]) (i) The congruence in question is soluble if and only if the congruence $4(x^2-x-1) = (2x-1)^2-5 \equiv 0 \pmod p$ is soluble. This in turn is soluble if and only if 5 is a quadratic residue modulo p. Hence, by hypothesis, the congruence $x^2 - x - 1 \equiv 0 \pmod p$ does indeed have a solution $\lambda \pmod p$.
(ii) With $\mu = 1 - \lambda$, one has

$$\mu^2 - \mu - 1 = (1 - 2\lambda + \lambda^2) - (1 - \lambda) - 1 = \lambda^2 - \lambda - 1 \equiv 0 \pmod p.$$

So μ is indeed a solution of $x^2 - x - 1 \equiv 0 \pmod p$. Moreover, if one were to have $\lambda \equiv \mu = 1-\lambda \pmod p$, then $2\lambda \equiv 1 \pmod p$, and hence $4(\lambda^2-\lambda-1) = (2\lambda-1)^2-5 \equiv -5 \not\equiv 0 \pmod p$, yielding a contradiction. So $\lambda \not\equiv \mu \pmod p$, as desired.
(iii) Since $(\lambda - \mu) \mid (\lambda^n - \mu^n)$, of course, one sees that u_n is an integer. Also, plainly, neither λ nor μ is equal to 0. Thus

$$u_0 = \frac{\lambda^0 - \mu^0}{\lambda - \mu} = 0 \quad \text{and} \quad u_1 = \frac{\lambda - \mu}{\lambda - \mu} = 1.$$

Moreover, using the fact that λ and μ both satisfy $x^2 - x - 1 \equiv 0 \pmod p$, we obtain

$$\lambda^{n+2} - \mu^{n+2} \equiv (\lambda + 1)\lambda^n - (\mu + 1)\mu^n \pmod p.$$

Since $p \nmid (\lambda - \mu)$, moreover, we see that

$$u_{n+2} \equiv (\lambda - \mu)^{-1}((\lambda^{n+1} - \mu^{n+1}) + (\lambda^n - \mu^n)) \equiv u_{n+1} + u_n \pmod p.$$

(c) (2+3 marks; [B]) Fermat's Little Theorem: Let p be a prime number, and suppose that $(a,p)=1$. Then one has $a^{p-1}\equiv 1 \pmod p$.

Proof: When $(a,p)=1$, the map $a\mapsto ax \pmod p$ permutes the residues $\{1,\dots,p-1\}$. Thus

$$a^{p-1}\prod_{i=1}^{p-1} i=\prod_{i=1}^{p-1}(ai)\equiv\prod_{i=1}^{p-1} i \pmod p.$$

Since $\prod_1^{p-1} i$ is coprime to p, it follows that $a^{p-1}\equiv 1 \pmod p$, completing the proof.

(d) (6 marks; [U]) From (b)(iii), we have $F_1\equiv 1\equiv u_1 \pmod p$ and

$$F_2=1=1+0\equiv u_1+u_0\equiv u_2 \pmod p.$$

Suppose that $F_n\equiv u_n \pmod p$ for $2\le n<N$. Then

$$F_N\equiv F_{N-1}+F_{N-2}\equiv u_{N-1}+u_{N-2}\equiv u_N \pmod p.$$

Then it follows by induction that $F_n\equiv u_n \pmod p$ for $n\ge 1$. But by Fermat's Little Theorem, whenever $(p-1)\mid n$, say $n=m(p-1)$, one has

$$u_n\equiv(\lambda-\mu)^{-1}((\lambda^m)^{p-1}-(\mu^m)^{p-1})\equiv(\lambda-\mu)^{-1}(1-1)\equiv 0 \pmod p.$$

Thus $F_n\equiv u_n\equiv 0 \pmod p$ whenever $(p-1)\mid n$.

2. (25 marks total)

(a) (2+2 marks; [B+H]) (i) Lagrange's Theorem: Let $f(x)\in\mathbb{Z}[x]$ have degree n (modulo p), with $n\ge 1$. Then the congruence $f(x)\equiv 0 \pmod p$ has at most n solutions.

(ii) We have $f(x)=(x-1)^2+7$, and so $f(x)\equiv 0 \pmod{11}$ if and only if $(x-1)^2\equiv -7\equiv 4 \pmod{11}$, whence $x\equiv 3$ or -1 modulo 11.

(b) (2+3+3 marks; [B+H+U$\sim$H]) (i) Hensel's Lemma: Let $f(x)\in\mathbb{Z}[x]$. Suppose that $f(a)\equiv 0 \pmod{p^j}$, and that $p^\tau \parallel f'(a)$. Then if $j\ge 2\tau+1$, it follows that (1) whenever $b\equiv a \pmod{p^{j-\tau}}$, one has $f(b)\equiv f(a) \pmod{p^j}$ and $p^\tau\parallel f'(b)$; (2) there exists a unique residue $t \pmod p$ with the property that $f(a+tp^{j-\tau})\equiv 0 \pmod{p^{j+1}}$. [acceptable to quote this with $\tau=0$]

(ii) Consider first the solution $x_0=3$ of $f(x_0)\equiv 0 \pmod{11}$. We have $f'(x)=2x-2$, so that $f'(3)\equiv 4 \pmod{11}$. Thus $11^0\parallel f'(3)$. Note that $3\cdot 4\equiv 1 \pmod{11}$, so that $4^{-1}\equiv 3 \pmod{11}$. Then Hensel's lemma shows that there is the unique solution

$$x_1\equiv 3-f(3)(f'(3))^{-1}\equiv 3-11\cdot 3\equiv -30\equiv 91 \pmod{121}$$

to the congruence $f(x)\equiv 0 \pmod{121}$ corresponding to x_0. Similarly, when $x_0=-1$, we obtain the unique solution

$$x_1\equiv -1-f(-1)(f'(-1))^{-1}\equiv -1-11\cdot(-3)\equiv 32 \pmod{121}.$$

(iii) Since $f(x)=(x-1)^2+7$, the congruence $f(x)\equiv 0 \pmod{49}$ implies first that $7\mid(x-1)$, and hence that $7\equiv 0 \pmod{49}$. Thus we derive a contradiction, showing that there are no solutions of this congruence.

(c) (6 marks; [U]) The only solution of $f(x) \equiv f'(x) \equiv 0 \pmod{p}$ is $x \equiv 1 \pmod{p}$, since $f'(x) = 2x - 2$ and $(p, 2) = 1$. But $f(1) = 1 - 2 + 8 = 7$, so that for such values of x one has $f(x) \equiv 0 \pmod{p}$ if and only if $7 \mid p$. But $p > 7$, and hence any solution $x \pmod{p}$ of $f(x) \equiv 0 \pmod{p}$ satisfies $f'(x) \not\equiv 0 \pmod{p}$. But then Hensel's lemma shows that every solution of the congruence $f(x) \equiv 0 \pmod{p}$ lifts uniquely to a corresponding solution modulo p^n. By Lagrange's theorem, there are $z \leq 2$ solutions of the congruence $f(x) \equiv 0 \pmod{p}$, and these lift uniquely to z solutions modulo p^n. Thus there are at most 2 solutions modulo p^n.

(d) (2+5 marks; [H]+[U∼H]) (i) Plainly, one has $x \equiv 0 \pmod{2}$, say $x = 2y$. On substituting, we find that $4y^2 - 4y + 8 \equiv 0 \pmod{8}$, whence $y^2 - y + 2 \equiv 0 \pmod{2}$. But this congruence is satisfied for every integer y as a simple application of Fermat's Little Theorem, for example. Then $f(x) \equiv 0 \pmod{8}$ has solutions $x \equiv 0, 2, 4, 6 \pmod{8}$.

(ii) Let p be either 70001 or 70003. Then if $f(x) \equiv 0 \pmod{p}$, one has $(x - 1)^2 \equiv -7 \pmod{p}$, whence $\left(\dfrac{-7}{p}\right) = 1$. But by invoking quadratic reciprocity, one finds that

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)(7-1)/4} \left(\frac{p}{7}\right) = \left(\frac{p}{7}\right).$$

The quadratic residues modulo 7 are $1^2 \equiv 6^2 \equiv 1$, $2^2 \equiv 5^2 \equiv 4$ and $3^2 \equiv 4^2 \equiv 2 \pmod{7}$, and thus

$$\left(\frac{-7}{70001}\right) = \left(\frac{70001}{7}\right) = \left(\frac{1}{7}\right) = 1$$

and

$$\left(\frac{-7}{70003}\right) = \left(\frac{70003}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Then there are no solutions of $f(x) \equiv 0 \pmod{560024}$, since 70003 divides the modulus, and there are no solutions modulo 70003. When $p = 70001$, meanwhile, there are precisely two solutions, say a and b, of the congruence $f(x) \equiv 0 \pmod{p}$. But for each $c \in \{a, b\}$, and $d \in \{0, 2, 4, 6\}$, it follows from the Chinese Remainder Theorem that there exists an integer y with $y \equiv c \pmod{p}$ and $y \equiv d \pmod{8}$. But $f(y) \equiv f(c) \equiv 0 \pmod{p}$ and $f(y) \equiv f(d) \equiv 0 \pmod{8}$, so that $f(y) \equiv 0 \pmod{2^3 \cdot p}$. Moreover, by examining these solutions modulo 8 and modulo p, one sees that each such y is distinct modulo $8p$. Thus there are $2 \times 4 = 8$ solutions of $f(x) \equiv 0 \pmod{560024}$ distinct modulo 560024.

3. (25 marks total)

(a) (2+2 marks; [B+B]) (i) The Euler totient $\phi(n)$ is given by

$$\phi(n) = n \prod_{p|n} (1 - 1/p),$$

where the product is taken over the distinct prime divisors of n.

Euler's Theorem: If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(b) (2+2 marks; [B]) (i) A residue g modulo n is a primitive root when the order of g modulo n is $\phi(n)$.

(ii) Primitive roots modulo n exist if and only if $n = 1$, 2, 4, p^α or $2p^\alpha$, wherein p denotes an odd prime number. [No loss of credit if 1 is missed]

(c) (4+4 marks; [U∼H+U]) (i) If $x^n \equiv 1 \pmod{pq}$, then $g_1^n \equiv 1 \pmod{p}$. Write $n = h(p-1)+r$ with $0 \le r < p-1$. Then it follows from Fermat's Little Theorem (a special case of Euler's theorem) that $g_1^n = (g_1^{p-1})^h g_1^r \equiv g_1^r \pmod{p}$. But g_1 is primitive, and $0 \le r < p-1$, and thus $r = 0$ and $(p-1) \mid n$. The relation $(q-1) \mid n$ follows symmetrically.

(ii) By the Chinese Remainder Theorem, there exists an integer w with $w \equiv g_1 \pmod{p}$ and $w \equiv g_2 \pmod{q}$. But then whenever $w^n \equiv 1 \pmod{pq}$, one has $(p-1) \mid n$ and $(q-1) \mid n$, so that $[p-1, q-1] \mid n$. Hence, the order of w is divisible by the least common multiple of $p-1$ and $q-1$, and cannot be any smaller. But writing $[p-1, q-1] = m(p-1) = l(q-1)$, one sees that

$$w^{m(p-1)} \equiv (w^{p-1})^m \equiv 1 \pmod{p}$$

and

$$w^{l(q-1)} \equiv (w^{q-1})^l \equiv 1 \pmod{q},$$

by Fermat's Little Theorem, and hence $w^{[p-1,q-1]} \equiv 1 \pmod{pq}$, by the Chinese Remainder Theorem. So the order of $w \pmod{pq}$ is precisely $[p-1, q-1]$.

(d) (5+4 marks; [U]) (i) If $a^{pq+1} \equiv 1 \pmod{pq}$ for all integers a with $(a, pq) = 1$, then by (c)(i) one has $(p-1) \mid (pq+1)$, whence $(p-1) \mid (q+1)$. By symmetry, also $(q-1) \mid (p+1)$.

(ii) Thus $p-1 \le q+1$ and $q-1 \le p+1$, so that $p-2 \le q \le p+2$. But p and q are distinct and odd, so that $p-2 = q$ or $q = p+2$. Thus $|p-q| = 2$. Since $p < q$ and $(q-1) \mid (p+1)$, it follows that $q = p+2$. The relation $(p-1) \mid (q+1)$ then gives

$$\frac{q+1}{p-1} = \frac{p+3}{p-1} = 1 + \frac{4}{p-1} \in \mathbb{Z},$$

whence $p-1 \in \{1,2,4\}$. But p is odd, so $p = 3$ or 5.

4. (25 marks total)

(a) (2+3 marks; [B]) The rational number

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n],$$

where p_n and q_n are relatively prime integers with $q_n \ge 1$, is the n^{th} convergent to θ. Thus

$$p_0/q_0 = [a_0] = a_0/1, \quad \text{so that} \quad p_0 = a_0 \quad \text{and} \quad q_0 = 1,$$

and

$$p_1/q_1 = [a_0; a_1] = a_0 + 1/a_1 = (a_0a_1+1)/a_1 \quad \text{so that} \quad p_1 = a_0a_1+1 \quad \text{and} \quad q_1 = a_1.$$

(b) (2+5 marks; [B+B]) Dirichlet's Theorem: Let θ be a real number. Then whenever Q is a real number exceeding 1, there exist integers p and q with $1 \le q < Q$ and $(p,q) = 1$ such that $|q\theta - p| \le 1/Q$.

Proof: Write $N = \lceil Q \rceil$, and consider the $N+1$ real numbers 0, 1, $\{\theta\}$, $\{2\theta\}$, $\ldots$, $\{(N-1)\theta\}$. These $N+1$ numbers all lie in the unit interval $[0,1]$, so by the Box Principle, at least two must lie in one of the N intervals of the shape $[h/N, (h+1)/N]$ for $h = 0, 1, \ldots, N-1$. The difference between these two numbers has the shape $q\theta - p$ with p and q integers satisfying $0 < |q| \le N-1$. It follows that integers p and q may be chosen with $1 \le q < Q$ and $|q\theta - p| \le 1/N \le 1/Q$. The coprimality condition on p and q follows by dividing through by (p,q).

(c) (2+4 marks; [B+B]) (i) (a) A number θ is algebraic if there is a polynomial $f \in \mathbb{Z}[t]$ of positive degree having the property that $f(\theta) = 0$. (b) A complex number θ is transcendental if it is not algebraic of any degree.

(b) Liouville's Theorem: Suppose that θ is an algebraic number of degree $d > 1$. Then there exists a positive number $c = c(\theta)$ such that whenever q is a natural number, and p is an integer, one has $|\theta - p/q| \geq c/q^d$.

(d) (7 marks; [U, somewhat $\sim$H]) Write $\theta = \sum_1^\infty 2015^{-(b_n+1)n!}$. For each natural number j, write $q_j = 2015^{(b_j+1)j!}$ and

$$p_j = 2015^{(b_j+1)j!} \sum_{n=1}^{j} 2015^{-(b_n+1)n!}.$$

Then when j is large, p_j and q_j are natural numbers satisfying $(p_j, q_j) = 1$, since all prime divisors of q_j divide 2015, and $p_j \equiv 1 \pmod{2015}$. Further, one has

$$|\theta - p_j/q_j| = \sum_{n=j+1}^{\infty} 2015^{-(b_n+1)n!} < 2015^{1-(j+1)!} < q_j^{-j/10}.$$

If θ were algebraic, then it would be algebraic of some degree $d \geq 1$. By Liouville's theorem, for some positive number c, one would have $|\theta - p/q| \geq c/q^d$ for every pair of natural numbers p and q with $(p, q) = 1$ and q sufficiently large. But the above upper bound contradicts this lower bound as soon as $j > 10d$ and j is large enough in terms of c. Hence θ is transcendental.

5. (25 marks total)

(a) (2+2 marks; [B+U∼H]) An arithmetical function f is said to be multiplicative if (a) f is not identically zero, and (b) whenever $(m, n) = 1$, one has $f(mn) = f(m)f(n)$. Suppose that $f(n)$ is multiplicative, and write $g(n) = f(n^3)$. Then whenever $m, n \in \mathbb{N}$ satisfy $(m, n) = 1$, we have $g(mn) = f(m^3n^3)$ with $(m^3, n^3) = (m, n)^3 = 1$, so that $g(mn) = f(m^3)f(n^3) = g(m)g(n)$. Then $g(mn) = g(m)g(n)$, and since $g(1) = f(1) \neq 0$, the multiplicativity of g follows.

(b) (3+3 marks; [U∼H]) (i) One has $\tau(p^h) = h + 1$ (since $1, p, p^2, \dots, p^h$ are the positive divisors of p^h), and hence $\tau(p^{3h}) = 3h + 1$. But for every non-negative integer h, one has $3h + 1 \leq (h + 1)^2$, and hence $\tau(p^{3h}) \leq \tau(p^h)^2$.

(ii) Since $\tau(n)$ is multiplicative, it follows that $\tau(n^3)$ is multiplicative. Thus, by multiplicativity, one has

$$\tau(n^3) = \prod_{p^h \| n} \tau(p^{3h}) \leq \prod_{p^h \| n} \tau(p^h)^2 = \tau(n)^2.$$

Thus $\tau(n^3) \leq \tau(n)^2$, as required.

(c) (6 marks; [B∼H]) One has

$$\begin{aligned}\sum_{1 \leq n \leq x} \sqrt{\tau(n^3)} \leq \sum_{1 \leq n \leq x} \tau(n) &= \sum_{1 \leq n \leq x} \sum_{d | n} 1 = \sum_{1 \leq d \leq x} \sum_{1 \leq m \leq x/d} 1 \\ &= \sum_{1 \leq d \leq x} \lfloor x/d \rfloor = x \sum_{1 \leq d \leq x} 1/d + O(x) = x \log x + O(x).\end{aligned}$$

(d) (5+4 marks; [B+U]) (i) Möbius inversion formula: Let f be any arithmetical function, and define $g(n) = \sum_{d|n} f(d)$. Then one has $f(n) = \sum_{d|n} \mu(d)g(n/d)$.

Proof: Define the arithmetic function $\nu(n)$ to be 1 when $n = 1$, and otherwise to be 0. Given that $g(n) = \sum_{d|n} f(d)$, one obtains

$$\begin{aligned}\sum_{d|n} \mu(d)g(n/d) &= \sum_{d|n} \sum_{e|(n/d)} \mu(d)f(e) = \sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d) \\ &= \sum_{e|n} f(e)\nu(n/e) = f(n).\end{aligned}$$

(ii) When n is the prime power p^h with $h \geq 1$, one has

$$\sum_{d|n} 3^{\omega(d)} = \sum_{l=0}^{h} 3^{\omega(p^l)} = 1 + \sum_{l=1}^{h} 3 = 3h + 1 = \tau(p^{3h}).$$

Thus, by multiplicativity, one has

$$\sum_{d|n} 3^{\omega(d)} = \prod_{p^h \| n} \tau(p^{3h}) = \tau(n^3).$$

Thus, applying the Möbius inversion formula, one obtains

$$\sum_{d|n} \mu(d)\tau((n/d)^3) = 3^{\omega(n)},$$

so that the duality $d \leftrightarrow n/d$ of divisors yields

$$\sum_{d|n} \mu(n/d)\tau(d^3) = 3^{\omega(n)}.$$

End of solutions.