PURDUE UNIVERSITY

Department of Mathematics

INTRODUCTION TO NUMBER THEORY

MA 49500 and MA 59500 – SOLUTIONS

13th December 2023   120 minutes

This paper contains **EIGHT** *questions worth a total of* **200 points**.
All EIGHT answers will be used for assessment.
Calculators, textbooks, notes and cribsheets are **not** *permitted in this examination.*

Do not turn over until instructed.

1. [4+4+4+4+4+4+4+4+4+4=40 points] Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with "T", and those which may be false with "F".

a. The congruence $x^4 \equiv 1 \pmod{16}$ has precisely 4 distinct solutions modulo 16.

Solution: FALSE (Each of the 8 integers 1, 3, 5, 7, 9, 11, 13, 15 are solutions for x).

b. There exist integers x and y having the property that $2023x + 97y = 1$.

Solution: TRUE (the integer 97 is prime, and since $97 \nmid 2023$ we see that $(2023, 97) = 1$, whence the Euclidean Algorithm confirms that the equation $2023x+97y = 1$ has a solution in integers x, y).

c. The integer $n! + 1$ is composite for infinitely many positive integers n.

Solution: TRUE (take $n = p - 1$ with $p \geq 5$ prime, and apply Wilson's theorem to see that $n! \equiv -1 \pmod{p}$, whence $p|(n! + 1)$ and it follows that $n! + 1$ is composite).

d. The Euler totient $\varphi(n)$ is a multiplicative function of n.

Solution: TRUE (this is a basic result from the course).

e. The integer 2 is a primitive root modulo 31.

Solution: FALSE (observe that $2^5 \equiv 1 \pmod{31}$, so that 2 has order dividing 5, which is less than 30, whence 2 cannot be a primitive root modulo 31).

f. Let p be an odd prime. Then the congruence $x^{p-1} + 1 \equiv 0 \pmod{p^2}$ has precisely $p - 1$ solutions modulo p^2.

Solution: FALSE (if the congruence has any solution x, then $p \nmid x$, and hence it follows from Fermat's Little Theorem that $x^{p-1} + 1 \equiv 1 + 1 = 2 \pmod{p}$, and since p is odd we conclude that $x^{p-1} + 1 \not\equiv 0 \pmod{p^2}$).

g. Let p be an odd prime, and suppose that a and b are both quadratic non-residues modulo p. Then ab is a quadratic non-residue modulo p.

Solution: FALSE (if a and b are both quadratic non-residues modulo p, then we have $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, so that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^2 = 1$ and ab is a quadratic residue).

h. Let p be an odd prime number, and suppose that g is a primitive root modulo p. Then g is a quadratic non-residue.

Solution: TRUE (by Euler's criterion, we have $\left(\frac{g}{p}\right) \equiv g^{(p-1)/2} \not\equiv 1 \pmod{p}$, since the order of g modulo p is $p - 1$, and hence $\left(\frac{g}{p}\right) = -1$ and g is a quadratic non-residue).

i. Suppose that the real number θ has continued fraction expansion $[2; 1, 2, 1, 4, 1, 6, 1, 8, \ldots]$. Then θ is a quadratic irrational number.

Solution: FALSE (if θ is a quadratic irrational real number, then it has an ultimately periodic continued fraction expansion, and hence θ is not quadratic irrational).

j. The equation $x^2 - 2023y^2 = 1$ has infinitely many solutions in integers x and y.

Solution: TRUE (since 2023 is not a square, it follows from the theory of Pell's equation that this equation has infinitely many solutions in x and y).

Continued...

2. [5+5+5+5+5+5=30 points]

(a) Define the *least common multiple* of two non-zero integers a and b.

Solution: Non-zero integers a and b have a common multiple m when $a|m$ and $b|m$. The *least common multiple* of a and b is the smallest positive common multiple of these integers.

(b) Define the *order* of a reduced residue a modulo n.

Solution: The order of a modulo n is the smallest positive integer d satisfying the property that $a^d \equiv 1 \pmod{n}$.

(c) Let n be a positive odd integer. Define the *Jacobi symbol* $\left(\frac{a}{n}\right)$.

Solution: Let Q be a positive odd integer, and suppose that $Q = p_1 \dots p_s$, where the p_i are prime numbers (not necessarily distinct). Then we define the **Jacobi symbol** $\left(\frac{a}{Q}\right)$ as follows:

(i) $\left(\frac{a}{1}\right) = 1$; (ii) $\left(\frac{a}{Q}\right) = 0$ whenever $(a, Q) > 1$;

(iii) $\left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)$ whenever $(a, Q) = 1$.

(d) Define the *partial quotients* of the continued fraction expansion of a real number θ.

Solution: If the continued fraction expansion of θ is $[a_0; a_1, a_2, \ldots]$, then the integers a_i are the *partial quotients* of θ.

(e) Define what it means for a real number α to be *transcendental*.

Solution: The real number θ is **transcendental** if θ is **not** algebraic of any degree. That is, the number θ is not the root of any non-zero polynomial having rational coefficients.

(f) Let d be a positive integer which is not a perfect square. Define the *fundamental solution* of the Pell equation $x^2 - dy^2 = 1$.

Solution: The unique solution (x, y) of the equation $x^2 - dy^2 = 1$ in which x and y have their smallest positive values is called the **fundamental solution**.

3. [4+7+7+7=25 points] For what values of n do primitive roots modulo n exist? (Provide as complete a list as you are able, without justifying your answer).

Solution: 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 and $\alpha \in \mathbb{N}$.

(b) Let p be an odd prime, and suppose that g is a primitive root modulo p^2. By considering the solutions of the congruence $x^2 \equiv 1 \pmod{p^2}$, prove that

$$g^{p(p-1)/2} \equiv -1 \pmod{p^2}.$$

Solution: Put $x = g^{p(p-1)/2}$, and observe that one then has $x^2 = g^{p(p-1)} \equiv 1 \pmod{p^2}$, as a consequence of Euler's Theorem. But then $(x+1)(x-1) \equiv 0 \pmod{p^2}$. One has $(x+1, x-1) = (x+1, 2)|2$, so that p (an odd prime) cannot divide both $x+1$ and $x-1$. Thus we see that $x \equiv \pm 1 \pmod{p^2}$. But since g is primitive, it has order $\phi(p^2) = p(p-1)$, and hence $g^{p(p-1)/2} \not\equiv 1 \pmod{p^2}$. Thus we deduce that $x = g^{p(p-1)/2} \equiv -1 \pmod{p^2}$, as required.

Continued...

(c) Let p be an odd prime, and let a be an integer with $(a,p)=1$. Show that when the congruence $x^2 \equiv a \pmod{p^2}$ has a solution, then

$$a^{p(p-1)/2} \equiv 1 \pmod{p^2},$$

and when the congruence $x^2 \equiv a \pmod{p^2}$ has no solution, then

$$a^{p(p-1)/2} \equiv -1 \pmod{p^2}.$$

Solution: Suppose that $(a,p)=1$. When the congruence $x^2 \equiv a \pmod{p^2}$ has a solution, then $(x,p)=1$, and one has $a^{p(p-1)/2} \equiv x^{p(p-1)} \equiv 1 \pmod{p^2}$, as a consequence of Euler's Theorem. This confirms the first assertion. Suppose next that the congruence $x^2 \equiv a \pmod{p^2}$ has no solution. Let g be a primitive root modulo p^2. Then there exists an integer r for which $g^r \equiv a \pmod{p^2}$, and r must be odd for otherwise the congruence $x^2 \equiv a \pmod{p^2}$ would be soluble. Put $r=2s+1$. Then, again by Euler's Theorem, one has $a^{p(p-1)/2} \equiv g^{sp(p-1)+p(p-1)/2} \equiv g^{p(p-1)/2} \pmod{p^2}$. Hence, by part (i), one has $a^{p(p-1)/2} \equiv -1 \pmod{p^2}$ in this case, confirming the second assertion.

(d) Let p be an odd prime, and define

$$\left[\frac{a}{p^2}\right] = \begin{cases} +1, & \text{when } (a,p)=1 \text{ and } x^2 \equiv a \pmod{p^2} \text{ has a solution,} \\ -1, & \text{when } (a,p)=1 \text{ and } x^2 \equiv a \pmod{p^2} \text{ has no solution,} \\ 0, & \text{when } p|a. \end{cases}$$

Prove that $\left[\frac{a}{p^2}\right] \equiv a^{p(p-1)/2} \pmod{p^2}$, and hence deduce that

$$\left[\frac{-1}{p^2}\right] = (-1)^{(p-1)/2} \quad \text{and} \quad \left[\frac{ab}{p^2}\right] = \left[\frac{a}{p^2}\right]\left[\frac{b}{p^2}\right].$$

Solution: First, since p is odd, one has $p(p-1)/2 \geq 3$. Thus, when $p|a$ one finds that $a^{p(p-1)/2} \equiv 0 \pmod{p^2}$. Then when $p|a$ one has

$$\left[\frac{a}{p^2}\right] \equiv 0 \equiv a^{p(p-1)/2} \pmod{p^2}.$$

When $(a,p)=1$, meanwhile, then by applying (c)(ii), one sees directly that

$$\left[\frac{a}{p^2}\right] \equiv a^{p(p-1)/2} \pmod{p^2}.$$

The conclusion follows on noting that, since $p^2>2$, the congruence $\left[\frac{a}{p^2}\right] \equiv \pm 1 \pmod{p^2}$ implies that $\left[\frac{a}{p^2}\right] = \pm 1$. Hence, since p is odd, one finds that

$$\left[\frac{-1}{p^2}\right] \equiv (-1)^{p(p-1)/2} = (-1)^{(p-1)/2}$$

implies that $\left[\frac{-1}{p^2}\right] = (-1)^{(p-1)/2}$, and likewise

$$\left[\frac{ab}{p^2}\right] \equiv (ab)^{p(p-1)/2} \equiv a^{p(p-1)/2} b^{p(p-1)/2} \equiv \left[\frac{a}{p^2}\right]\left[\frac{b}{p^2}\right] \pmod{p^2}$$

implies that $\left[\frac{ab}{p^2}\right] = \left[\frac{a}{p^2}\right]\left[\frac{b}{p^2}\right] \pmod{p^2}$.

Continued...

4. [4+8+8=20 points] (a) State a version of Hensel's lemma.

Solution: Hensel's Lemma: Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(a) \equiv 0 \pmod{p^j}$, and that $p^\tau \| f'(a)$. Then if $j \geq 2\tau + 1$, it follows that (1) whenever $b \equiv a \pmod{p^{j-\tau}}$, one has $f(b) \equiv f(a) \pmod{p^j}$ and $p^\tau \| f'(b)$; (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 $\tau = 0$]

(b) Let p be an odd prime. Show that the congruence

$$x^p - 2x + 1 \equiv 0 \pmod{p}$$

has precisely one solution modulo p, and determine that solution.

Solution: By Fermat's Little theorem, for any integer x, one has

$$x^p - 2x + 1 \equiv x - 2x + 1 = -x + 1 \pmod{p}.$$

Thus, the congruence in question has the solution given by $x \equiv 1 \pmod{p}$, and no other solutions.

(c) Let p be an odd prime number, and let j be an integer with $j \geq 2$. Determine the number of solutions of the congruence

$$x^p - 2x + 1 \equiv 0 \pmod{p^j}.$$

Justify your answer.

Solution: The congruence in question has only the solution $x \equiv 1 \pmod{p}$ when $j = 1$. Write $f(t) = t^p - 2t + 1$. Then $f'(t) = pt^{p-1} - 2$ and so, since p is odd, one has $f'(1) \equiv -2 \not\equiv 0 \pmod{p}$. Then $p^0 \| f'(1)$, and by Hensel's Lemma, for every $j \geq 2$, the solution $x = 1$ of the congruence modulo p lifts uniquely to a solution modulo p^j. Then there is precisely one solution modulo p^j to the congruence in question.

5. [4+8+5+8=25 points] (a) State, without proof, the Law of Quadratic Reciprocity for the Legendre symbol.

Solution: Quadratic Reciprocity: Let p and q be distinct odd prime numbers. Then

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

(b) Determine the primes p for which 5 is a quadratic residue modulo p.

Solution: If 5 is to be a quadratic residue modulo p, 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 $p \equiv \pm 1 \pmod{5}$.

(c) Show that when k is a natural number, then $5k+2$ must be divisible by a prime number p satisfying $p \equiv \pm 2 \pmod 5$.

Solution: All prime numbers except 5 take the shape either $5n \pm 1$ or $5n \pm 2$, for integral n. The integer $5k+2$ is not divisible by 5. If it were divisible only by primes of the shape $5n \pm 1$, then one would have $5k+2 \equiv \pm 1 \pmod 5$, which is impossible. Thus $5k+2$ must be divisible by at least one of the remaining class of primes of the shape $5n \pm 2$, proving the claim.

(d) Show that the Diophantine equation

$$y^2 = x(5x^2 + 2) + 5$$

has no solution in integers x and y.

Solution: Suppose by way of deriving a contradiction that (x, y) is an integral solution of this equation. Since 5 is not a square, the equation has no solution with $x = 0$. When x is non-zero, meanwhile, the term $x(5x^2 + 2)$ is a multiple of an integer of the shape $5k + 2$, and hence (part (c)) is divisible by an odd prime p satisfying $p \equiv \pm 2 \pmod 5$. But then $y^2 \equiv 5 \pmod p$, so that y is a quadratic residue modulo p. By (b), meanwhile, this is possible only when $p \equiv \pm 1 \pmod 5$, yielding a contradiction. Then the equation in question has no integral solutions.

6. [10+10=20 points] (a) Suppose that $a(n)$ and $b(n)$ are multiplicative functions. Show that the arithmetic function $c(n) = \sum_{d|n} a(n/d)b(d)$ is also multiplicative.

Solution: Suppose that $a(n)$ and $b(n)$ are multiplicative. Then whenever $m, n \in \mathbb{N}$ satisfy $(m, n) = 1$, we have $a(mn) = a(m)a(n)$ and $b(mn) = b(m)b(n)$, whence

$$c(mn) = \sum_{d|mn} a(nm/d)b(d) = \sum_{e|n} \sum_{f|m} a\left(\frac{n}{e}\frac{m}{f}\right) b(ef).$$

Since the values of e and f in the latter summation are necessarily coprime, we find that

$$\begin{aligned} c(mn) &= \sum_{e|n} \sum_{f|m} a(n/e)a(m/f)b(e)b(f) \\ &= \left(\sum_{e|n} a(n/e)b(e)\right)\left(\sum_{f|m} a(m/f)b(f)\right) = c(m)c(n). \end{aligned}$$

Thus $c(n)$ is indeed a multiplicative function.

(b) Show that $\sigma(n) = \sum_{d|n} \varphi(n/d)\tau(d)$.

Solution: For each prime power p^h one has

$$\begin{aligned} \sum_{j=0}^{h} \phi(p^{h-j})\tau(p^j) &= \sum_{j=0}^{h-1} (p^{h-j} - p^{h-j-1})(j+1) + \phi(p^0)\tau(p^h) \\ &= p^h + p^{h-1} + \cdots + p - h + h + 1 = \sum_{d|p^h} d = \sigma(p^h), \end{aligned}$$

and so

$$\sigma(p^h) = \sum_{d|p^h} \phi(p^h/d)\tau(d).$$

Thus it follows from multiplicativity that $\sigma(n) = \sum_{d|n} \phi(n/d)\tau(d)$ for $n \in \mathbb{N}$.

Continued...

7. [10+10=20 points] Define the arithmetic function $\sigma_{-1} : \mathbb{N} \to \mathbb{R}$ by putting
$$\sigma_{-1}(n) = \sum_{d|n} \frac{1}{d}.$$

(a) Find an asymptotic formula for the average
$$\frac{1}{x} \sum_{1\le n\le x} \sigma_{-1}(n).$$

Solution: One has
$$\sum_{1\le n\le x} \sigma_{-1}(n) = \sum_{1\le n\le x} \sum_{d|n} \frac{1}{d} = \sum_{1\le d\le x} \frac{1}{d} \sum_{1\le m\le x/d} 1 = \sum_{1\le d\le x} \frac{1}{d} \left\lfloor \frac{x}{d} \right\rfloor$$
$$= x \sum_{1\le d\le x} \frac{1}{d^2} + O\left(\sum_{1\le d\le x} \frac{1}{d} \right) = x \sum_{d=1}^{\infty} \frac{1}{d^2} + O\left(x \sum_{d>x} \frac{1}{d^2} \right) + O(\log x),$$
and hence
$$\frac{1}{x} \sum_{1\le n\le x} \sigma_{-1}(n) = \frac{6}{\pi^2} + O\left(\frac{\log x}{x} \right).$$

(b) By using multiplicativity, prove that $\varphi(n)\sigma_{-1}(n) \le n$ for all natural numbers n.

Solution: Observe that whenever p is prime and $h \ge 0$, one has
$$\varphi(p^h)\sigma_{-1}(p^h) = p^h(1 - 1/p)\left(1 + p^{-1} + \ldots + p^{-h}\right) = p^h(1 - p^{-h-1}) \le p^h.$$
Hence, making use of the multiplicative properties of $\varphi(n)$, $\sigma(n)$ and n, we deduce that for each natural number n one has
$$\varphi(n)\sigma_{-1}(n) = \prod_{p^h \| n} \varphi(p^h)\sigma_{-1}(p^h) \le \prod_{p^h \| n} p^h = n.$$

8. [4+8+8=20 points] (a) State Dirichlet's Theorem on Diophantine approximation.

Solution: 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 $|q\theta - p| \le 1/Q$.

(b) Obtain the continued fraction expansion of the quadratic irrational $\sqrt{11}$.

Solution: One has
$$\begin{aligned} [\sqrt{11}] &= 3, \quad 1/(\sqrt{11} - 3) = (\sqrt{11} + 3)/2, \\ [(\sqrt{11} + 3)/2] &= 3, \quad 1/((\sqrt{11} + 3)/2 - 3) = 2/(\sqrt{11} + 3 - 6) = \sqrt{11} + 3, \\ [\sqrt{11} + 3] &= 6, \quad 1/(\sqrt{11} + 3 - 6) = (\sqrt{11} + 3)/2, \end{aligned}$$
and we obtain repetition. Thus $\sqrt{11} = [3; \overline{3, 6}]$.

(c) Find the fundamental solution of the Pell equation $x^2 - 11y^2 = 1$, and hence write down a formula that describes all integer solutions of this Pell equation.

Solution: The continued fraction for $\sqrt{11}$ has periodic tail with period 2, so the fundamental solution is given by the the convergent $p_1/q_1 = 3 + 1/3 = 10/3$. Thus, we use the fundamental solution $(x, y) = (10, 3)$ (giving $10^2 - 11 \cdot 3^2 = 1$), and then deduce that all solutions (x, y) are determined via the relation $x + y\sqrt{11} = \pm(10 + 3\sqrt{11})^n$ $(n \in \mathbb{Z})$.

End of examination.