

MATHEMATICS DEPARTMENT  
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: TOPICS IN NUMBER THEORY

Model Solution No: 1

**Note:** Parts (a)–(d) are bookwork. Part (e) is a simplification of bookwork. Part (f) is unseen.

- a)  $g$  has order  $d$  modulo  $p$  if  $g^d \equiv 1 \pmod{p}$ , but  $g^{d_1} \not\equiv 1 \pmod{p}$  for any  $1 \leq d_1 < d$ .
- b) Suppose  $g$  has order  $d$  modulo  $p$  and that  $g^m \equiv 1 \pmod{p}$ . Write  $m = qd + r$  where  $0 \leq r < d$ . Then

$$g^r = g^{m-qd} = g^m(g^d)^{-q} \equiv 1 \pmod{p}.$$

By definition of order,  $r = 0$ . Hence  $d \mid m$ .

- c) Suppose  $g_1, g_2$  respectively have orders  $d_1$  and  $d_2$  where  $\gcd(d_1, d_2) = 1$ . Now

$$(g_1 g_2)^{d_1 d_2} \equiv (g_1^{d_1})^{d_2} (g_2^{d_2})^{d_1} \equiv 1 \pmod{p}.$$

Let  $d$  be the order of  $g_1 g_2$  modulo  $p$ . Then  $d \mid d_1 d_2$ . Moreover

$$g_1^d g_2^d \equiv 1 \pmod{p}$$

thus

$$(g_1^{d_1})^d g_2^{d_1 d} \equiv 1 \pmod{p}$$

and so

$$g_2^{d_1 d} \equiv 1 \pmod{p}.$$

Hence  $d_2 \mid d_1 d$ . As  $d_1$  and  $d_2$  are coprime,  $d_2 \mid d$ . Similarly  $d_1 \mid d$ , and so  $d_1 d_2 \mid d$ . Hence  $d = d_1 d_2$ .

- d)  $g$  is a primitive root modulo  $p$  if  $g$  has order  $p - 1$ .
- e) Factor  $p - 1$  as a product of powers of distinct primes:

$$p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}.$$

Now

$$x^{q_i^{e_i}} \equiv 1 \pmod{p}$$

has  $q_i^{e_i}$  incongruent solutions, whereas

$$x^{q_i^{e_i-1}} \equiv 1 \pmod{p}$$

has  $q_i^{e_i-1}$  incongruent solutions. Hence there is some  $g_i$  satisfying

$$g_i^{q_i^{e_i}} \equiv 1 \pmod{p}, \quad g_i^{q_i^{e_i-1}} \not\equiv 1 \pmod{p}.$$

## MA 3H1

It follows that  $g_i$  has order  $q_i^{e_i}$  modulo  $p$ . Let  $g = g_1 g_2 \cdots g_r$ . By the previous part of the question,  $g$  has order

$$\prod q_i^{e_i} = p - 1$$

and hence is a primitive root.

- f) By the numerical observations, 5 has order 37 modulo 149, and 44 has order 4 modulo 149. Hence  $220 \equiv 71 \pmod{149}$  has order  $4 \times 37 = 149 - 1$ . Hence 71 is a primitive root modulo 149.

MATHEMATICS DEPARTMENT  
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: TOPICS IN NUMBER THEORY

Model Solution No: 2

**Note:** Parts (a),(b) are bookwork. Part (c) is unseen. Part (d) is unseen but similar to a homework problem.

a) Let  $a$  be an integer and  $p$  an odd prime. If  $p \mid a$  then

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

Hence suppose that  $p \nmid a$ . Let  $g$  be a primitive root modulo  $p$ . We know that  $a \equiv g^r \pmod{p}$  for some  $0 \leq r \leq p-2$ .

We will show first that  $r$  is even if and only if  $a$  is a quadratic residue. Clearly if  $r$  is even then  $a$  is a quadratic residue. Suppose that  $a$  is a quadratic residue. Then  $a \equiv u^2 \pmod{p}$  and  $u \equiv g^s \pmod{p}$ . Thus  $g^{r-2s} \equiv 1 \pmod{p}$  and so  $(p-1) \mid (r-2s)$ . But  $p-1$  is even and so  $r$  must be even.

Now, regardless of whether  $r$  is odd or even,

$$a^{(p-1)/2} \equiv (g^{(p-1)/2})^r \equiv (-1)^r = \left(\frac{a}{p}\right) \pmod{p}.$$

b) First Supplement to the Law of Quadratic Reciprocity:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Second Supplement to the Law of Quadratic Reciprocity

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

c) Let  $x$  be even. Suppose  $p$  is a prime,  $p \mid (x^4 + 1)$ . Thus  $p$  is odd and  $p \nmid x$ . Now

$$-1 \equiv x^4 \pmod{p}$$

and hence

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

Moreover,  $x^4 + 1 = (x^2 + 1)^2 - 2x^2$ , so

$$2x^2 \equiv (x^2 + 1)^2 \pmod{p},$$

## MA 3H1

and so

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

Hence

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

By the first supplement,  $p \equiv 1 \pmod{4}$ , and by the second  $p \equiv 1, 7 \pmod{8}$ . But if  $p \equiv 7 \pmod{8}$  then  $p \equiv 3 \pmod{4}$  which is impossible. Thus  $p \equiv 1 \pmod{8}$ .

- d) Suppose that there are finitely many primes congruent to 1 modulo 8 and let these be  $p_1, p_2, \dots, p_n$ . Let  $x = 2p_1p_2 \cdots p_n$ , and let  $p$  be a prime divisor of  $x^4 + 1$ . Then  $p \neq p_i$  and  $p \equiv 1 \pmod{8}$  by the (c) giving a contradiction.

MATHEMATICS DEPARTMENT  
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: TOPICS IN NUMBER THEORY

Model Solution No: 3

**Note:** Parts (a),(b),(c) are bookwork. Part (d) is similar to, but harder than, a homework question.

- a) **(Blichfeldt's Theorem)**. Let  $m \geq 1$  be an integer. Let  $S$  be a subset of  $\mathbb{R}^n$  with volume  $V(S)$  satisfying

$$V(S) > m.$$

There exist  $m + 1$  distinct points  $\mathbf{x}_0, \dots, \mathbf{x}_m \in S$  such that

$$\mathbf{x}_j - \mathbf{x}_i \in \mathbb{Z}^n, \quad \text{for } 0 \leq i, j \leq m.$$

**(Minkowski's Theorem)**. Let  $\Lambda$  be a sublattice of  $\mathbb{Z}^n$  of index  $m$ . Let  $C$  be a convex symmetric subset of  $\mathbb{R}^n$  having volume  $V(C)$  satisfying

$$V(C) > 2^n m.$$

Then  $C$  and  $\Lambda$  have a common point other than  $\mathbf{0}$ .

- b) Let

$$S = \frac{1}{2}C = \left\{ \frac{1}{2}\mathbf{x} : \mathbf{x} \in C \right\}.$$

The volume of  $S$  is

$$V(S) = \frac{1}{2^n} V(C) > m.$$

By Blichfeldt's Theorem, there are  $m + 1$  distinct points  $\mathbf{x}_0, \dots, \mathbf{x}_m \in S$  such that

$$\mathbf{x}_j - \mathbf{x}_i \in \mathbb{Z}^n, \quad \text{for } 0 \leq i, j \leq m.$$

Let  $\mathbf{y}_j = \mathbf{x}_j - \mathbf{x}_0 \in \mathbb{Z}^n$  for  $j = 0, \dots, m$ . These are  $m + 1$  distinct points  $\mathbf{y}_j$  in  $\mathbb{Z}^n$  and  $\Lambda$  has  $m$  cosets in  $\mathbb{Z}^n$ . So two distinct  $\mathbf{y}_i, \mathbf{y}_j$  lie in the same coset of  $\Lambda$ . Thus,  $\mathbf{x}_j - \mathbf{x}_i = \mathbf{y}_j - \mathbf{y}_i$  is a non-zero element of  $\Lambda$ . Now we can write  $\mathbf{x}_j = \mathbf{c}/2$  and  $\mathbf{x}_i = \mathbf{c}'/2$  where  $\mathbf{c}$  and  $\mathbf{c}'$  are in  $C$ . Hence

$$\frac{\mathbf{c} - \mathbf{c}'}{2}$$

is a non-zero element of  $\Lambda$ . Now  $C$  is symmetric so,  $-\mathbf{c}' \in C$  as well as  $\mathbf{c} \in C$ . Finally  $C$  is convex and  $(\mathbf{c} - \mathbf{c}')/2$  is the mid-point between  $\mathbf{c}$  and  $-\mathbf{c}'$ , so it must be in  $C$  as well as being a non-zero element of  $\Lambda$ . This is the point whose existence is asserted in the statement of the theorem.

c) Let

$$E_{a,b} = \left\{ (x, y) \in \mathbb{R}^2 : \frac{x^2}{a^2} + \frac{y^2}{b^2} < 1 \right\}.$$

The area of the ellipse is given by the double integral

$$V(E_{a,b}) = \iint_{E_{a,b}} 1 dx dy.$$

To evaluate this double integral we'll use a substitution. Let  $u = x/a$  and  $v = y/b$ . Then the ellipse  $E_{a,b}$  in the  $xy$ -plane becomes the unit disc

$$D = \{(u, v) \in \mathbb{R}^2 : u^2 + v^2 < 1\}$$

in the  $uv$ -plane. Moreover  $dx = d(au) = a du$  and  $dy = d(bv) = b dv$ . Hence

$$V(E_{a,b}) = \iint_D ab du dv = ab \iint_D 1 du dv = ab V(D),$$

and  $V(D) = \pi$  is the area of the unit disc  $D$ . We obtain

$$V(E_{a,b}) = \pi ab.$$

d) Let

$$\Lambda = \{(x, y) \in \mathbb{Z}^2 : x \equiv \lambda y \pmod{N}\}.$$

It is clear that  $\Lambda$  is a sublattice of index  $N$ . Let

$$C = \{(x, y) \in \mathbb{R}^2 : x^2 + 2y^2 < 2N\}.$$

We can rewrite this as

$$x^2/2N + y^2/N < 1.$$

This is a convex symmetric subset of area  $\pi\sqrt{N}\sqrt{2N} = \pi\sqrt{2}N$ . Note that

$$\pi\sqrt{2}N > 4N,$$

since  $\pi^2 > 9 > 8 = (4/\sqrt{2})^2$ . Hence we can apply Minkowski's Theorem. From that we get that there is a non-zero  $(x, y) \in \Lambda \cap C$ . Hence  $x^2 + 2y^2 < 2N$ . Moreover,  $x \equiv \lambda y \pmod{N}$  and so  $x^2 \equiv 2y^2 \pmod{N}$ . Hence  $N \mid (x^2 - 2y^2)$ . As  $\sqrt{2}$  is irrational and  $(x, y)$  is non-zero,  $x^2 - 2y^2 \neq 0$ . But  $|x^2 - 2y^2| \leq x^2 + 2y^2 < 2N$  so  $x^2 - 2y^2 = \pm N$ .

MATHEMATICS DEPARTMENT  
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: TOPICS IN NUMBER THEORY

Model Solution No: 4

**Note:** Part (a) is an exercise set in class. Part (b) is bookwork. Parts (c) and (d) are similar to homework problems.

a) Note

$$\frac{d^n}{dX^n}(X^r) = \begin{cases} r(r-1)\cdots(r-n+1)X^{r-n} & r \geq n \\ 0 & r < n. \end{cases}$$

To prove the result we must show that  $n! \mid r(r-1)\cdots(r-n+1)$ . But

$$\frac{r(r-1)\cdots(r-n+1)}{n!} = \binom{r}{n} \in \mathbb{Z}$$

as required.

b) By Taylor's Theorem

$$f(a+x) = f(a) + f'(a)x + \frac{f^{(2)}(a)}{2!}x^2 + \cdots + \frac{f^{(n)}(a)}{n!}x^n$$

where  $n$  is the degree of  $f$  (note that all higher derivatives vanish). We want  $b$  to satisfy two conditions, one of them that  $b \equiv a \pmod{p^m}$ . Let us write  $b = a + p^m y$  where the integer  $y$  will be determined later. Then

$$f(b) = f(a) + p^m f'(a)y + p^{2m}(\text{integer}).$$

Since  $f(a) \equiv 0 \pmod{p^m}$  we have  $f(a) = p^m c$  where  $c$  is an integer. Thus

$$f(b) = p^m(c + f'(a)y) + p^{2m}(\text{integer}).$$

Note that  $p^{m+1} \mid p^{2m}$ . To make  $f(b) \equiv 0 \pmod{p^{m+1}}$  it is enough to choose  $y$  so that  $p \mid (c + f'(a)y)$ . In other words, we want  $y$  so that  $f'(a)y \equiv -c \pmod{p}$ . But  $f'(a) \not\equiv 0 \pmod{p}$  and so is invertible modulo  $p$ . Let  $h$  satisfy  $hf'(a) \equiv 1 \pmod{p}$ . Then we choose  $y = -hc$  and take  $b = a - hcp^m$  and then both required congruences are satisfied.

- c) Note  $\left(\frac{3}{5}\right) = -1$ , so  $x^2 \equiv 3 \pmod{5^3}$  does not have solutions, so the system of simultaneous congruences does not have solutions.
- d) To solve  $y^3 \equiv 3 \pmod{5^3}$ , we solve first  $y^3 \equiv 3 \pmod{5}$ . Running through the residue classes we see that  $y \equiv 2 \pmod{5}$ . Now write  $y = 2 + 5t$ . Then

$$(2 + 5t)^3 \equiv 3 \pmod{25}$$

## MA 3H1

and so

$$60t \equiv 20 \pmod{25}$$

so

$$3t \equiv 1 \pmod{5},$$

so  $t \equiv 2 \pmod{5}$  and hence  $y \equiv 12 \pmod{25}$ . Now write  $y = 12 + 25t$ . Then

$$(12 + 25t)^3 \equiv 3 \pmod{125},$$

so

$$3 \times 12^2 \times 25t \equiv 25 \pmod{125}$$

so

$$3 \times 12^2 t \equiv 1 \pmod{5},$$

so  $t \equiv 3 \pmod{5}$  and hence  $y \equiv 87 \pmod{125}$ . By the Chinese Remainder Theorem, the two congruences

$$y \equiv 87 \pmod{125}, \quad y \equiv 1 \pmod{4}$$

have a unique solution modulo  $4 \times 125 = 500$ . By inspection, this is  $y \equiv 87 + 2 \times 125 = 337 \pmod{500}$ .

MATHEMATICS DEPARTMENT  
FOURTH YEAR UNDERGRADUATE EXAMS

Course Title: TOPICS IN NUMBER THEORY

Model Solution No: 5

**Note:** Parts (a),(b),(c) are bookwork. Part (d)(i) is similar to a homework problem. Part (d)(ii) is unseen. Part d(iii) is in the homework.

- a) If  $\alpha = 0$  define  $\text{ord}_p(\alpha) = \infty$  and  $|\alpha|_p = 0$ . Otherwise, write  $\alpha = p^u a/b$  where  $a, b \in \mathbb{Z}$  and  $p \nmid a, b$ . Define  $\text{ord}_p(\alpha) = u$  and  $|\alpha|_p = p^{-u}$ .
- b) This is clear if either  $\alpha$  or  $\beta$  is zero, so suppose they're both non-zero. Write

$$\alpha = p^u \frac{a}{b}, \quad \beta = p^v \frac{c}{d},$$

where  $p$  does not divide  $a, b, c, d$ . Without loss of generality,  $u \leq v$ . Then

$$\alpha + \beta = p^u \frac{ad + p^{v-u}bc}{cd}.$$

Note  $ad + p^{v-u}bc$  is an integer, so we can write,  $ad + p^{v-u}bc = p^\ell a'$  where  $\ell \geq 0$  and  $p \nmid a'$ . Moreover,  $p \nmid cd$ . Hence

$$\text{ord}_p(\alpha + \beta) = u + \ell \geq u = \min\{\text{ord}_p(\alpha), \text{ord}_p(\beta)\}.$$

Finally,

$$-\text{ord}_p(\alpha + \beta) \leq -\min\{\text{ord}_p(\alpha), \text{ord}_p(\beta)\} = \max\{-\text{ord}_p(\alpha), -\text{ord}_p(\beta)\},$$

which implies that

$$|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}.$$

- c) Write  $s_n = a_1 + a_2 + \cdots + a_n$ . The series  $\sum a_i$  converges iff the sequence of partial sums  $\{s_n\}$  converges. This happens iff the sequence  $\{s_n\}$  is  $p$ -adically Cauchy. Now if  $m \geq n$  then

$$|s_m - s_n|_p = |a_{n+1} + a_{n+2} + \cdots + a_m|_p \leq \max\{|a_{n+1}|_p, \dots, |a_m|_p\}.$$

If  $\lim_{n \rightarrow \infty} |a_n|_p = 0$ , then  $|s_m - s_n|_p \rightarrow 0$  as  $m, n \rightarrow \infty$ . Hence the sequence  $\{s_n\}$  is Cauchy as required. Conversely, suppose the sequence  $\{s_n\}$  is Cauchy, and write  $m = n - 1$ . Then

$$|s_n - s_{n-1}|_p = |a_n|_p$$

and so  $\lim_{n \rightarrow \infty} |a_n|_p = 0$ .

- d) (i) This converges if and only if  $\lim |(21/2)^{2n}|_p = 0$ . This will be the case iff  $|21/2|_p < 1$ , which is true exactly for  $p = 3, 7$ .
- (ii) Suppose  $n = kp + 1$ . Then  $|n|_p = 1$ , and so  $|n^n|_p = 1$ . Hence  $\sum n^n$  does not converge for any  $p$ .