NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Sean Lim Wei Xinq, Loh Bo Huai Victor, Goh Jun Le

MA3265 Introduction to Number Theory
Sem 2 AY 09/10

Question 1

Let x be the cents and y be the dollars of the inital amount on the check. We can form the following equation:

$$3(100y + x) = 100x + y - 59$$

This is equivalent to solving the Diophantine equation

$$299a + 97b = -59$$

where $a = y$ and $b = -x$.

By the Euclidean algorithm, we have

$$\begin{aligned} 299 &= 3(97) + 8 \\ 97 &= 12(8) + 1 \end{aligned}$$

Working backwards, we have

$$\begin{aligned} 97 - 12(8) &= 1 \\ 97 - 12(299 - 3(97)) &= 1 \\ 37(97) - 12(299) &= 1 \end{aligned}$$

Multiplying each term by 59 gives us a particular solution $a_0 = 708$ and $b_0 = -2183$. Furthermore, we have the following equations:

$$\begin{aligned} a &= a_0 + 97t \\ b &= b_0 - 299t \end{aligned}$$

where $t \in \mathbb{Z}$. Given the constraint that $0 \leq x, y < 100$, we find that $0 \leq 708 + 97t < 100$. This means that $t = -7$ and hence $x = 90$ and $y = 29$.

Question 2

(a) Let $x = \sqrt{d}$ and we have the continued fraction

$$x = 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{\ddots}}}}$$

Rewriting gives us

$$x = 3 + \cfrac{1}{3 + \cfrac{1}{3 + 3 + \cfrac{1}{3 + \cfrac{1}{\ddots}}}}$$

Therefore we have

$$x = 3 + \frac{1}{3 + \frac{1}{3+x}}$$

Solving the equation, we have

$$\begin{aligned} x &= 3 + \frac{3+x}{10+3x} \\ (10+3x)x &= 3(10+3x) + 3 + x \\ 10x + 3x^2 &= 33 + 10x \\ x^2 &= 11 \\ d &= 11 \end{aligned}$$

(b) We want to solve the Pell's equation

$$x^2 - 11y^2 = 1$$

We know that

$$h_n^2 - dk_n^2 = (-1)^{n-1} q_{n+1}$$

So we need to find a suitable n such that n is odd and $q_{n+1} = 1$. We start with $n = 1$. We have $\xi_1 = -3 + \sqrt{11}$. So we have $q_1 = 1$.

Next, $h_1 = a_1 h_0 + h_{-1} = 3(a_0 h_{-1} + h_{-2}) + h_{-1} = 3(3) + 1 = 10$ and $k_1 = a_1 k_0 + k_{-1} = a_1(a_0 k_{-1} + k_{-2}) = 3(1) = 3$. So our solution is $x = 10$ and $y = 3$, and we can check that

$$10^2 - 11(3)^2 = 1$$

Question 3

(a) We have

$$\begin{aligned} \left(\frac{-7}{p}\right) &= 1 \\ \Leftrightarrow \left(\frac{7}{p}\right) = \left(\frac{-1}{p}\right) &= \pm 1 \end{aligned}$$

By quadratic reciprocity we have the two cases

$$\left(\frac{p}{7}\right)(-1)^{3(p-1)/2} = 1 = \left(\frac{-1}{p}\right) \text{ or } \left(\frac{p}{7}\right)(-1)^{3(p-1)/2} = -1 = \left(\frac{-1}{p}\right)$$

For the first case, $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$. Therefore we have

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

which yields

$$p \equiv 1, 2, 4 \pmod 7$$

By the Chinese Remainder Theorem (CRT), we have

$$p \equiv 1, 9, 25 \pmod{28}$$

For the second case, if $\left(\frac{-1}{p}\right) = -1$ if and only if $p \equiv 3 \pmod 4$. Therefore we again have

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

which yields

$$p \equiv 1, 2, 4 \pmod 7$$

By the CRT, we have

$$p \equiv 11, 15, 23 \pmod{28}$$

Combining, we have $p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$.

(b) Since $f(x, y) = az^2 + bxy + cy^2$ must be reduced we must have

$$0 < a \leq \sqrt{-\frac{d}{3}}$$

Now $d = -7$ implies that $a = 1$. Then $b = 0, 1$. If $b = 0$, then $-4c =$ odd, giving a non-integer solution for c which cannot happen. So $b = 1$ and we have

$$1 - 4c = -7 \Rightarrow c = 2$$

Therefore the only reduced binary quadratic form is

$$f(x, y) = x^2 + xy + 2y^2$$

as desired.

(c) Firstly, if $p = 2$ then observe that $2 = 0^2 + (0)(1) + 2(1)^2$. So assume that p is odd.

By Theorem 34 in the helpsheet, if p is a prime represented by f then

$$x^2 \equiv -7 \pmod{4p}$$

has a solution. Since p is odd, we have $(4, p) = 1$ and therefore

$$x^2 \equiv -7 \equiv 1 \pmod 4$$

and

$$x^2 \equiv -7 \pmod p$$

By (a) we have $p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$.

Question 4

Notice that $f(x, xz) = (1 - z)f(x, z)$. This means that

$$\sum_{n=0}^{\infty} a_n(x)x^n z^n = \sum_{n=0}^{\infty} a_n(x)z^n - \sum_{n=0}^{\infty} a_n(x)z^{n+1}$$

Furthermore, since $f(x, 0) = 1$ implies that $a_0 = 1$, comparing the coefficient of z^n and we obtain:

$$a_n(x)x^n = a_n(x) - a_{n-1}(x)$$

So we have

$$a_n(x) = \frac{a_{n-1}(x)}{1 - x^n}$$

and we are done.

Question 5

(a) We will prove by induction. Firstly, consider the equation

$$x^2 \equiv 1 \pmod p$$

By Theorem 12, there are at most two solutions. But the two solutions are 1 and -1, and hence there are exactly two solutions. Now let $f(x) = x^2 - 1$. So $f'(x) = 2x$ and $f'(\pm 1) = \pm 2$. Since p is an odd prime, it follows that $p \nmid f'(\pm 1)$. So by Hensel's Lemma, there exists a total of 2 solutions lifted from ± 1. These two solutions are again, ± 1 by inspection.

Now suppose that there are two exactly solutions, namely ± 1 for the equation

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

Then, again, $f'(\pm 1) = \pm 2$ and so $p \nmid f'(\pm 1)$ and therefore by Hensel's Lemma, ± 1 will be lifted to exactly two solutions, namely ± 1 by inspection and we are done.

(b) We again prove by induction. Let $\alpha = 3$ and consider the equation

$$x^2 \equiv 1 \pmod 8$$

Firstly, consider the equation

$$x^2 \equiv 1 \pmod 2$$

By inspection there is only one solution: $x \equiv 1 \pmod 2$. Now $f'(1) = 2$ and observe that $2 \mid f'(1)$ and $2 \mid f(1)/2$, hence 1 is lifted to two solutions - $1 + 0(2) = 1 \pmod p$ and $1 + 1(2) = 3 \equiv -1 \pmod p$. Next, we have $f'(\pm 1) = \pm 2 \equiv 2 \pmod 4$. So again, $2 \mid f'(\pm 1)$ and $2 \mid f(\pm 1)/2^2$. So ± 1 are each lifted to two solutions.

1 is lifted to $1 + 0(4) = 1$ and $1 + 1(4) = 5 = 1 + 2^{3-1}$.

-1 is lifted to $-1 + 0(2) = -1$ and $-1 + 1(2) = 1 = -1 + 2^{3-1}$.

Now consider the equation

$$x^2 \equiv 1 \pmod{2^{\alpha-1}}$$

and suppose that there are four solutions, namely $1, 1 + 2^{\alpha-2}, -1, -1 + 2^{\alpha-2}$. We want to use this to solve

$$x^2 \equiv 1 \pmod{2^\alpha}$$

Now we have

$$f'(\pm 1) = \pm 2$$
$$f'(\pm 1 + 2^{\alpha-2}) = \pm 2 + 2^{\alpha-1}$$

Now 2 divides both $f'(\pm 1)$ and $f'(\pm 1 + 2^{\alpha-2})$. We also have

$$f(\pm 1) = 0 f(\pm 1 + 2^{\alpha-2}) = \pm 2^{\alpha-1} + 2^{2\alpha-4}$$

So $p \mid f(\pm 1)/2^{\alpha-1}$ and so, ± 1 is lifted to two solutions each.

1 is lifted to $1 + 0(2^{\alpha-1}) = 1$ and $1 + 1(2^{\alpha-1}) = 1 + 2^{\alpha-1}$.

-1 is lifted to $-1 + 0(2^{\alpha-1}) = -1$ and $-1 + 1(2^{\alpha-1}) = -1 + 2^{\alpha-1}$.

Next, $f(\pm 1 + 2^{\alpha-2})/2^{\alpha-1} = \pm 2^{\alpha-1} + 2^{2\alpha-4}/2^{\alpha-1} = \pm 1 + 2^{\alpha-3}$.

So $2 \nmid f(\pm 1 + 2^{\alpha-2})$, and therefore, there are no solutions. So the solutions to the equation

$$x^2 \equiv 1 \pmod \alpha$$

are $1, 1 + 2^{\alpha-1}, -1$ and $-1 + 2^{\alpha-1}$ and this completes the proof.

Question 6

If there are no m such that $m^k \mid n$, then

$$\sum_{d^k \mid n} \mu(d) = \mu(1) = 1$$

Now let $p_1, p_2, \cdots, p_t$ be the primes such that $p_i^k \mid n$ for all i. Then we have

$$\begin{aligned}\sum_{d^k \mid n} \mu(d) &= \mu(1) + \sum_{i=1}^{t} \mu(p_i) + \sum_{1 \le i < j \le t} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \cdots p_t) \\ &= 1 - t + \binom{t}{2} - \binom{t}{3} + \cdots + (-1)^t \binom{t}{t} \\ &= (1 + (-1))^t = 0\end{aligned}$$

as required.

Question 7

(a) Observe that if $x^2 = (-x)^2$. So there are at most $\frac{p-1}{2}$ squares mod p. Then, suppose $x^2 \equiv y^2 \pmod{p}$. Then we have

$$\begin{aligned} & p \mid (x^2 - y^2) \\ \Rightarrow & p \mid (x-y)(x+y) \\ \Rightarrow & p \mid (x-y) \text{ or } p \mid (x+y)\end{aligned}$$

If $p \mid (x-y)$ then $x \equiv y \pmod{p}$, and if $p \mid (x+y)$ then $x \equiv -y \pmod{p}$, and this shows that there are at least $\frac{p-1}{2}$ squares mod p. Hence, $(\mathbb{Z}/p\mathbb{Z})^\times$ partitions equally into squares and non-squares. This implies that

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$$

Alternative proof:

Let $((\mathbb{Z}/p\mathbb{Z})^\times)^2$ be the set of quadratic residues modulo p. Claim 1: $((\mathbb{Z}/p\mathbb{Z})^\times)^2$ is a normal subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Proof of Claim 1. Let $a, b \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2$. Then there exists $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $a = x^2$ and $b = y^2$. Then we have

$$ab^{-1} = (x^2)(y^2)^{-1} = (x^2)(y^{-2}) = (xy^{-1})^2$$

Since $xy^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$, we can conclude that $ab^{-1} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2$ and hence, $((\mathbb{Z}/p\mathbb{Z})^\times)^2$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ and that it is normal since $(\mathbb{Z}/p\mathbb{Z})^\times$ is Abelian, and this proves the claim.

Claim 2: $[(\mathbb{Z}/p\mathbb{Z})^\times : ((\mathbb{Z}/p\mathbb{Z})^\times)^2] = 2$.

Proof of Claim 2. Let $C_2 := \{1, -1\}$ be the group of order 2 under multiplication. We define the map $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \to C_2$ by $x \mapsto \left(\frac{x}{p}\right)$. Let g be a primitive root modulo p. Note that g cannot be a square. Suppose it is. Then $g \equiv h^2 \pmod{p}$ for some $h \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then $g^{\frac{p-1}{2}} \equiv h^{p-1} \equiv 1 \pmod{p}$, which contradicts the fact that g is a primitive root. Hence, $\left(\frac{g}{p}\right) = -1$ and we see that the map is surjective.

Also, note that for all $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $\phi(xy) = \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \phi(x)\phi(y)$, showing that ϕ is a homomorphism. Next, observe that the kernel of ϕ are the squares of $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e. $\ker(\phi) = ((\mathbb{Z}/p\mathbb{Z})^\times)^2$. Hence, by the First Isomorphism Theorem we have

$$(\mathbb{Z}/p\mathbb{Z})^\times / ((\mathbb{Z}/p\mathbb{Z})^\times)^2 \cong C_2$$

and the claim thus follows.

Therefore, the set $(\mathbb{Z}/p\mathbb{Z})^\times$ is partitioned equally into squares and non-squares, and hence, the number of squares and non-squares modulo p are equal, which tells us that

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$$

(b) Claim: $\left(\frac{m}{p}\right) = 1$ if and only if $\left(\frac{-m}{p}\right) = 1$. Proof of Claim: We have

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

But $p \equiv 1 \pmod 4$ implies that $\left(\frac{-1}{p}\right) = 1$, therefore the claim follows.

So we have $\frac{p-1}{2}$ integers from 1 to $p-1$, and they form $\frac{p-1}{4}$ pairs of the form $(i, p-i)$ where each pair sums up to p. Hence

$$\sum_{\substack{m=1 \\ \left(\frac{m}{p}\right)=1}}^{p-1} m = p \cdot \frac{p-1}{4} = \frac{p(p-1)}{4}$$

and this completes the proof.

Question 8

(a) Observe that if $p \mid a$, then $p \mid b$ and vice versa, because $(a, b) = 1$.

Case 1: $p \mid a$ or $p \mid b$. Choose $x = 1$ and we are done.

Case 2: $p \nmid a$ and $p \nmid b$. Choose $x = 0$ and we are done.

Therefore in both cases, there exists an integer x with fulfils the requirements.

(b) We write $c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. As an extension of part (a), we can let $x \equiv 0 \pmod p$ or $x \equiv 1 \pmod p$ depending on whether p divides a. Therefore we have the following equations:

$$\begin{aligned} x &\equiv a_1 \pmod{p_1} \\ x &\equiv a_2 \pmod{p_2} \\ &\cdots \\ x &\equiv a_r \pmod{p_r} \end{aligned}$$

where $a_i = 0$ if p_i does not divide a and $a_i = 1$ if p_i divides a. By the Chinese Remainder Theorem, there exists an integer x such that $(a + bx, c) = 1$.

Question 9

(a) Firstly, n cannot be even since $2^n - 1$ is odd. So suppose n is odd and that there exists an n such that $n \mid (2^n - 1)$. Let p be the smallest prime dividing n. Note that p must be odd. Hence we have $p \mid (2^n - 1)$. This implies that

$$2^n \equiv 1 \pmod{p}$$

By Fermat's Little Theorem

$$2^{p-1} \equiv 1 \pmod{p}$$

Now let h be the order of 2 in $\mathbb{Z}/p\mathbb{Z}$. Then $h \mid n$ and $h \mid (p-1)$. Now let q be a prime dividing h. Then, $q \mid n$ and $q \mid p-1$, but $q \mid n$ implies that $p < q$ and $q \mid (p-1)$ implies that $q < p$, a contradiction.

So $n \nmid (2^n - 1)$.

(b) Firstly, n cannot be even since $2^n + 1$ is odd. Let p be the smallest prime dividing n. Note that p must be odd. Hence we have $p \mid (2^n + 1)$. This implies that

$$2^n \equiv -1 \pmod{p}$$

So

$$2^{2n} \equiv 1 \pmod{p}$$

Again, by Fermat's Little Theorem,

$$2^{p-1} \equiv 1 \pmod{p}$$

Let the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ be h. Then $h \mid 2n$ and $h \mid (p-1)$. Let q be the largest prime dividing h. If q is odd, then $q < p-1$ and $q \mid 2n$ implies that $q \mid n$, and hence, $p < q$, contradiction. So $q = 2$. So $h = 2^k$ for some k. Then $2^k \mid 2n$ and $2^{k-1} \mid n$. If $k > 1$ then n is even, contradiction. So $k = 1$ and hence, $h = 2$ and this gives us $p = 3$, and we are done.