NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Goh Jun Le

MA3265 Introduction to Number Theory

AY 2008/2009 Sem 2

Question 1

Let x denote the number of adults and y denote the number of children. We are to solve the following linear Diophantine equation:

$$\begin{aligned} 1.80x + 0.75y &= 30 \\ 12x + 5y &= 200, \end{aligned}$$

subject to the restriction that $x > y \geq 0$.

We apply the Euclidean algorithm to 12 and 5: $12 = 5 \cdot 2 + 2$, $5 = 2 \cdot 2 + 1$. Working backwards, we have that

$$1 = 5 - 2 \cdot 2 = 5 - 2(12 - 5 \cdot 2) = 12(-2) + 5(5).$$

So $200 = 12(-2 \cdot 200) + 5(5 \cdot 200) = 12(-400) + 5(1000)$. The given equation is then equivalent to

$$12(x + 400) + 5(y - 1000) = 0,$$

which has the following general solution: $x = 5k - 400$, $y = 1000 - 12k$, $k \in \mathbb{Z}$.

To satisfy $x > y$, we must have $5k - 400 > 1000 - 12k \Rightarrow 17k > 1400 \Rightarrow k > 82.4$. To satisfy $y \geq 0$, we must have $1000 - 12k \geq 0 \Rightarrow k \leq 83.3$. The only $k \in \mathbb{Z}$ satisfying these two inequalities is $k = 83$. Thus $x = 5 \cdot 83 - 400 = 15$ and $y = 4$.

We conclude that $15 + 4 = 19$ people were in attendance.

Question 2

First note that $\sqrt{41} + [\sqrt{41}] = \langle \overline{12, 2, 2} \rangle$ i.e. it has period $r = 3$.

We know that x/y is a convergent (denoted by h_i/k_i) of the continued fraction of $\sqrt{41}$. We also know that

$$h_{nr-1}^2 - 41k_{nr-1}^2 = (-1)^{nr-2}$$

for all $n \geq 1$.

We seek the smallest x and y, and that will correspond to the smallest possible $nr - 1$. $n = 2$ is the smallest n such that $(-1)^{nr-2} = 1$. Thus $x = h_{2 \cdot 3 - 1} = h_5$ and $y = k_{2 \cdot 3 - 1} = k_5$.

We now calculate k_5 by definition:

$$\begin{aligned} k_0 &= 1 \\ k_1 &= 2 \cdot 1 + 0 = 2 \\ k_2 &= 2 \cdot 2 + 1 = 5 \\ k_3 &= 12 \cdot 5 + 2 = 62 \\ k_4 &= 2 \cdot 62 + 5 = 129 \\ k_5 &= 2 \cdot 129 + 62 = 320. \end{aligned}$$

Either by definition of h_5 or by substituting $y = 320$ into $x^2 - 41y^2 = 1$ and solving, we get that $x = 2049$. Thus $x = 2049$ and $y = 320$ are the smallest positive integers satisfying $x^2 - 41y^2 = 1$.

Question 3

(a) It is easy to see that the desired holds for $n = 2$. Henceforth we consider $n > 2$.

We observe that if $1 \le k \le n$ and $(k, n) = 1$, then $1 \le n - k \le n$ and $(n - k, n) = 1$. We also claim that $k \ne n - k$. If $k = n - k$, we have $n = 2k$. Then $1 = (k, n) = (k, 2k) = k$, so $n = 2$. Contradiction.

Based on the above, we pair up the $\varphi(n)$ terms in LHS to get

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} k = \sum_{\substack{k=1 \\ (k,n)=1}}^{[n/2]} n = \frac{\varphi(n)}{2} n = \frac{n\varphi(n)}{2}$$

as desired.

(b) If $\varphi(p - 1)$ is odd, we must have $p - 1 = 1$ or 2. Since p is an odd prime, we have $p = 3$. -1 is the only primitive root modulo 3, so the desired holds if $\varphi(p - 1)$ is odd.

Suppose $\varphi(p - 1)$ is even. We observe that if k generates $(\mathbb{Z}/p\mathbb{Z})^*$, then k^{-1} generates $(\mathbb{Z}/p\mathbb{Z})^*$ as well. That is, if k is a primitive root, then k^{-1} is a primitive root as well.

In addition, if $k = k^{-1}$, we have $p \mid k^2 - 1$. By Euclid's lemma, either $p \mid k - 1$ or $p \mid k + 1$ i.e. $k = 1$ or -1. But 1 is not a primitive root, and neither is -1 (unless $p = 3$, which has been considered previously). It follows that $k \ne k^{-1}$ for all primitive roots k.

Thus we may pair each primitive root with its (distinct) inverse. Since $kk^{-1} = 1$, the product of the primitive roots modulo p is $1 = (-1)^{\varphi(p-1)}$. Thus the desired holds.

We are done.

Question 4

(a)

$$\begin{aligned}
-\frac{1}{23} \sum_{1 \le n < p} n \left(\frac{n}{23}\right) &= -\frac{1}{23}(1 + 2 + 3 + 4 - 5 + 6 - 7 + 8 + 9 - 10 - 11 + 12 \\
&\qquad + 13 - 14 - 15 + 16 - 17 + 18 - 19 - 20 - 21 - 22) \\
&= -\frac{1}{23}(-69) = 3.
\end{aligned}$$

Thus there are 3 reduced binary quadratic forms of discriminant 23.

(b) The 3 reduced binary quadratic forms are:

$$\begin{gathered}
2x^2 + xy + 3y^2 \\
2x^2 - xy + 3y^2 \\
x^2 + xy + 6y^2.
\end{gathered}$$

Question 5

By quadratic reciprocity,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{\frac{p-1}{2}}.$$

Now, $x^2 \equiv 3 \pmod p$ is solvable iff $(\frac{3}{p}) = 1$. That in turn holds iff

$$\begin{aligned}
&(-1)^{\frac{p-1}{2}} = -1 \text{ and } \left(\frac{p}{3}\right) = -1, \text{ or } (-1)^{\frac{p-1}{2}} = 1 \text{ and } \left(\frac{p}{3}\right) = 1 \\
\Leftrightarrow\ & p \not\equiv 1 \pmod 4 \text{ and } p \equiv 2 \pmod 3, \text{ or } p \equiv 1 \pmod 4 \text{ and } p \not\equiv 2 \pmod 3 \\
\Leftrightarrow\ & p \equiv -1 \pmod{12} \text{ or } p \equiv 1 \pmod{12}.
\end{aligned}$$

(To show ($\Rightarrow$) in the last equivalence, one has to bear in mind that p is odd, so $p \not\equiv 2, 8 \pmod{12}$, and p is prime, so $p \not\equiv 9 \pmod{12}$.) We are done.

Question 6

(a) If $1 \le n \le p-2$ and $(\frac{n}{p}) = 1$ and $(\frac{n+1}{p}) = 1$, then $\frac{1}{4}(1 + \frac{n}{p})(1 + \frac{n+1}{p}) = 1$. If $1 \le n \le p-2$ and $(\frac{n}{p}) \ne 1$ or $(\frac{n+1}{p}) \ne 1$, then either $1 + \frac{n}{p} = 0$ or $1 + \frac{n+1}{p} = 0$ so $\frac{1}{4}(1 + \frac{n}{p})(1 + \frac{n+1}{p}) = 0$. The desired follows.

(b)

$$\begin{aligned}
N &= \frac{1}{4}\sum_{n=1}^{p-2}\left(1 + \left(\frac{n}{p}\right)\right)\left(1 + \left(\frac{n+1}{p}\right)\right) \\
&= \frac{1}{4}\left[\sum_{n=1}^{p-2} 1 + \sum_{n=1}^{p-2}\left(\frac{n}{p}\right) + \sum_{n=1}^{p-2}\left(\frac{n+1}{p}\right) + \sum_{n=1}^{p-2}\left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right)\right] \\
&= \frac{1}{4}\left[(p-2) + \left(0 - \left(\frac{p-1}{p}\right) - \left(\frac{p}{p}\right)\right) + \left(0 - \left(\frac{1}{p}\right) - \left(\frac{p}{p}\right)\right) + \sum_{n=1}^{p-2}\left(\frac{n(n+1)}{p}\right)\right] \\
&= \frac{1}{4}\left[(p-2) - \left(\frac{-1}{p}\right) - 1 + \left(-1 - \left(\frac{(p-1)p}{p}\right) - \left(\frac{p(p+1)}{p}\right)\right)\right] \\
&= \frac{1}{4}\left[p - 4 - (-1)^{\frac{p-1}{2}}\right],
\end{aligned}$$

where in the last equality, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ by quadratic reciprocity.

Now if $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd so $N = \frac{1}{4}(p - 4 - (-1)) = \frac{p-3}{4}$. If $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ is even so $N = \frac{1}{4}(p - 4 - 1) = \frac{p-5}{4}$. We are done.

Question 7

(a) Let 1 denote the arithmetical function which is identically 1. We note that

$$\omega(n) = \sum_{d\,|\,n} \chi(d) = \sum_{d\,|\,n} \chi(n/d)$$

i.e. $\omega = 1 * \chi$. It follows that

$$\sum_{n=1}^{\infty} \frac{\omega(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(1 * \chi)(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

as desired.

(b)
$$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \prod_p \left(1 + \frac{2^{\omega(p)}}{p^s} + \frac{2^{\omega(p^2)}}{(p^2)^s} + \dots\right) = \prod_p \left(1 + \frac{2}{p^s} + \frac{2}{p^{2s}} + \dots\right).$$

(c) Define the arithmetical function f as follows: let $f(1) = 1$. If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then define

$$f(n) = \begin{cases} 1 & \text{if } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Let $s \in \mathbb{R}$. It is easy to check that $\frac{f(n)}{n^s}$ is multiplicative (in n). So $\sum \frac{f(n)}{n^s}$ can be expressed as an Euler product:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{(p^2)^s} + \dots\right) = \prod_p \left(1 + \frac{1}{p^s}\right).$$

Let p be a prime. By comparing coefficients, we see that

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

We take $\prod_p$ on both sides to get

$$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for all $s \in \mathbb{R}$. It follows that $2^\omega = f * 1$ i.e.

$$2^{\omega(n)} = \sum_{d \mid n} f(d) \cdot 1 = \sum_{d \mid n} f(d)$$

as desired.

Remark. Strictly speaking, it is necessary to check that $\sum \frac{f(n)}{n^s}$ is absolutely convergent before writing it as an Euler product. We have omitted that.

Question 8

(a) If $a = 1$, the result is trivial. Suppose $a > 1$. Consider the group $(\mathbb{Z}/(a^k - 1)\mathbb{Z})^*$, of order $\varphi(a^k - 1)$. Note that $a^k = 1 \in (\mathbb{Z}/(a^k - 1)\mathbb{Z})^*$. Also, for all $1 \le j < k$, $1 < a^j < a^k$ so $a^j \ne 1 \in (\mathbb{Z}/(a^k - 1)\mathbb{Z})^*$. Thus a has order k. By Lagrange's theorem for finite groups, $k \mid \varphi(a^k - 1)$ as desired.

(b) We write

$$\varphi(m) = m \prod_{q \mid m} \frac{q-1}{q}.$$

Since $p \mid \varphi(m)$ and $p \nmid m$, we have $p \mid \prod_{q \mid m} \frac{q-1}{q}$. So $p \mid \prod_{q \mid m}(q - 1)$. By Euclid's lemma, $p \mid q - 1$ for some $q \mid m$. We are done.

(c) Suppose there are only finitely many primes $q_1, \dots, q_k$ satisfying $q \equiv 1 \pmod p$. By (a), $p \mid \varphi((pq_1 \cdots q_k)^p - 1)$. Also, $p \nmid (pq_1 \cdots q_k)^p - 1$. By (b), there is a prime q dividing $(pq_1 \cdots q_k)^p - 1$ such that $q \equiv 1 \pmod p$. But $q_i \nmid (pq_1 \cdots q_k)^p - 1$ for $1 \le i \le k$, so $q \ne q_1, \dots, q_k$. Contradiction. We are done.