CUHK Department of Mathematics

Enrichment Programme for Young Mathematics Talents 2019

Number Theory and Cryptography (SAYT1114)

Quiz 2

- The total score for the quiz is $100 + 25$ (25 points for the bonus question).
- If you obtain X points, your score will be $\min(X, 100)$.
- Time allowed: 90 minutes.
- The use of calculator is allowed.
- Unless otherwise specified, all variables defined in the quiz paper are integers.
- The function φ is the Euler totient function.

Q1. (10 points) True or false. For each of the statements below, determine if it is true or false. You are **not** required to justify your answer.

(a) (2 points) There are infinitely many primes in the form of $1234k + 567$.

(b) (2 points) For any real number x, $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$.

(c) (2 points) There exists $M > 0$ such that $\varphi(n) \nmid n$ for all $n \geq M$.

(d) (2 points) If $4a \equiv 8b \pmod{30}$, then $3a \equiv b \pmod{5}$.

(e) (2 points) If $3a \equiv b \pmod{5}$, then $4a \equiv 8b \pmod{30}$.

Q2. (30 points) Prove the following results regarding the infinitude of primes.

(a) (6 points) Let $n > 0$ be in the form of $4k + 3$. Then n has a prime factor in the form of $4k' + 3$.

(b) (12 points) Using (a), show that there are infinitely many primes in the form of $4k + 3$.

(c) (12 points) Using (a) and the fact that each prime factor of $n^2 + 2$ must either be equal to 2 or $\equiv 1, 3 \pmod{8}$, show that there are infinitely many primes in the form of $8k+3$.

Q3. (15 points) Prove the following statements. The variables defined in this question are not assumed to be integers.

(a) (6 points) If $x, y \geq 0$, then $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor$.

(b) (9 points) $\frac{1}{5} \leq x - \lfloor x \rfloor < \frac{2}{5}$ if and only if $\lfloor 5x \rfloor = 5\lfloor x \rfloor + 1$.

Q4. (15 points) Compute the following using results from Lecture 6.

(a) (5 points) $\varphi(1960)$.

(b) (10 points) The number of integers in $[1, 256]$ not divisible by $10, 12,$ or 15.

Q5. (15 points) Prove the following statements.

(a) (6 points) Given a, b, c, m with c and m nonzero. Then $a \equiv b \pmod{m}$ if and only if $ac \equiv bc \pmod{mc}$.

(b) (9 points) Given a, b, p where p is a prime number. If $a^2 \equiv b^2 \pmod{p}$, then $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

Q6. (15 points) Consider the linear congruence $14x \equiv b \pmod{35}$.

(a) (3 points) Find $gcd(14, 35)$.

(b) (12 points) Find all the incongruent solutions mod 35 for the following values of b:

(i) (6 points) $b = 21$.

(ii) (6 points) $b = 12$.

Q7 (Bonus Question). (25 points) The Möbius μ ("mu") function $\mu : \mathbb{Z}^+ \longrightarrow \{-1, 0, 1\}$ is defined on the set of positive integers as follows:

$$\mu(n) = \begin{cases} 0, & \text{if } k^2 \mid n \text{ for some } k > 1 \\ (-1)^r, & \text{if } n \text{ is a product of } r \text{ distinct prime numbers} \end{cases}$$

As a special case, $\mu(1) = (-1)^0 = 1$ since 1 is a product of 0 distinct primes.

(a) (3 points) Compute $\mu(n)$ for $1 \leq n \leq 15$.

(b) (5 points) Prove that $\sum_{d|n} \varphi(d) = n$ for all $n > 0$. The summation on the left hand side is over all positive divisors d of n.

(c) (17 points) Let f and g be functions defined on the set of positive integers. Suppose g satisfies

$$g(n) = \sum_{d|n} f(d)$$

for all $n > 0$. The Möbius inversion formula asserts that

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$$

for all $n > 0$.

(i) (3 points) Using (b) and the Möbius inversion formula, show that

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}.$$

(ii) (5 points) Show that

$$\sum_{d|n} \mu(d) = \delta(n),$$

where $\delta(1) = 1$ and $\delta(n) = 0$ for $n \geq 2$.

(iii) (9 points) Let $F(n)$ be the number of pairs of integers (i, j) such that $1 \leq i, j \leq n$ and $gcd(i, j) = 1$. Show that

$$F(n) = \sum_{i=1}^{n} \mu(i) \left\lfloor \frac{n}{i} \right\rfloor^2.$$

(Hint: start by writing $F(n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \delta(gcd(i, j))$.)

The End