CUHK Department of Mathematics

Enrichment Programme for Young Mathematics Talents 2019

Number Theory and Cryptography (SAYT1114)

Final Examination

- The total score for the examination is $100 + 15$ (15 points for the bonus question).
- If you obtain X points, your score will be $\min(X, 100)$.
- Time allowed: $(135 + \varepsilon)$ minutes.
- The use of calculator is allowed.
- Unless otherwise specified, all variables defined in the exam paper are integers.
- The function φ is the Euler totient function.

Q1. (5 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) (1 point) $gcd(ab, c) \mid gcd(a, c)gcd(b, c)$ for all $a, b, c > 0$.

(b) (1 point) Let x be a real number. If $\lfloor nx \rfloor = n\lfloor x \rfloor$ for all $n > 0$, then x is an integer.

(c) (1 point) Let a and b be nonzero. Then there exist infinitely many *composite* numbers in the form of $ak + b$.

(d) (1 point) If $a, b < 2^{2019}$, then computing $gcd(a, b)$ using Euclidean algorithm takes at most 2019 steps.

(e) (1 point) Let p and q be two distinct primes in the form of $4k + 3$. Then there exist a and b such that $a^2 + b^2 = pq$.

Q2. (11 points) Consider the linear Diophantine equation $4488x + 5678y = 238$.

(a) (3 points) Using Euclidean algorithm, compute $gcd(4488, 5678)$.

(b) (8 points) Using the calculation in (a), find **all** solutions of the given equation.

Q3. (8 points) Let $a, b > 0$.

(a) (6 points) Suppose $gcd(a, b) = 1$ and ab is a perfect cube. Show that both a and b are perfect cubes.

(b) (2 points) If the condition $gcd(a, b) = 1$ is removed, can we still conclude that both a and b are perfect cubes? Explain.

Q4. (10 points)

(a) (2 points) Solve $3x \equiv 9 \pmod{12}$.

(b) (8 points) Find all the solutions of the following congruences

$$\begin{cases} x \equiv 3 & \pmod 5 \\ x \equiv 2 & \pmod 7 \\ 3x \equiv 9 & \pmod{12}. \end{cases}$$

Q5. (10 points) Using the fact that $164^2 \equiv -1 \pmod{2069}$, find a solution of $x^2+y^2 = 2069$. (Hint: The identity $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$ may be useful.)

Q6. (11 points) Let $n > 0$. Prove the following facts about $\varphi(n)$.

(a) (2 points) If n is even, then $\varphi(n) \leq \frac{n}{2}$.

(b) (6 points) If $n > 2$, then $\varphi(n)$ is even.
(Hint: either n has an odd prime factor, or $n = 2^k$ for some $k > 1$.)

(c) (3 points) If $n > 2$, then $\varphi(\varphi(n)) < \frac{n}{2}$. You can use the results of (a) and (b).

Q7. (15 points) Given an odd number $m > 1$.
If m is a prime, by Fermat's Little Theorem, we have

$$2^{m-1} \equiv 1 \pmod m.$$

Is the converse true, i.e. if $2^{m-1} \equiv 1 \pmod m$, does it follow that m is a prime? The answer is negative, and the smallest counter-example is $m = 341 = 31 \times 11$.
In this question, we are going to show that there are infinitely many (odd) composite numbers m such that $2^{m-1} \equiv 1 \pmod m$.

(a) (4 points) Show that $2^m - 1$ is composite if m is composite.

(b) (8 points) Let $n := 2^m - 1$. Show that, if $2^{m-1} \equiv 1 \pmod m$, then $2^{n-1} \equiv 1 \pmod n$.
(Hint: Note that $2^m \equiv 1 \pmod n$, so one just needs to show $m \mid (n-1)$.)

(c) (3 points) Using (a) and (b), finish the proof that there are infinitely many (odd) composite numbers m such that $2^{m-1} \equiv 1 \pmod m$.

Q8. (15 points) Given a positive integer n, let $s(n)$ be the number of incongruent solutions mod n of the equation $x^2 \equiv 1 \pmod{n}$.

For example, $s(12) = 4$ since $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$.

By Chinese Remainder Theorem, s is multiplicative; that is, if $gcd(m, n) = 1$ then $s(mn) = s(m)s(n)$. Therefore, it suffices to find $s(p^k)$ for primes p and positive integers k.

(a) (6 points) Let p be an odd prime and $k > 0$. Show that $s(p^k) = 2$.
(Hint: show that, if $x^2 \equiv 1 \pmod{p^k}$, then $x \equiv 1 \pmod{p^k}$ or $x \equiv -1 \pmod{p^k}$.)

(b) (9 points) It remains to consider $s(2^k)$ for $k = 1, 2, \ldots$.

  (i) (3 points) Compute $s(2)$ and $s(4)$.

  (ii) (6 points) Show that $s(2^k) = 4$ for $k \geq 3$.

(Notice that $s(n) \leq 2$ if and only if $n = 2, 4, p^k, 2p^k$, p is any odd prime. Does this look familiar? Indeed, there exists a primitive root mod n precisely when $n = 2, 4, p^k, 2p^k$. You can investigate further when you are home.)

Q9. (15 points) Let p be a prime greater than 3. For an integer a not divisible by p, let $\bar{a}$ denote the multiplicative inverse of a mod p^2 (**not** mod p).

(a) (3 points) For $p = 5$, show by explicit computation that $\bar{1} + \bar{2} + \bar{3} + \bar{4} \equiv 0 \pmod{25}$.

(b) (12 points) Consider the polynomial $Q(x) := (x-1)(x-2)\ldots(x-(p-1))$. If we write $Q(x) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 p + a_0$, it is known that $p \mid a_i$ for $1 \leq i \leq p-2$. (The proof is not difficult, but not required in this question.)

  (i) (2 points) Show that $a_0 = (p-1)!$.

  (ii) (7 points) By considering $Q(p)$, show that $p^2 \mid a_1$.

  (iii) (3 points) Hence, prove that $\bar{1} + \bar{2} + \cdots + \overline{p-1} \equiv 0 \pmod{p^2}$. This result is known as Wolstenholme's theorem.

Q10 (Bonus Question). (15 points) Given $n > 0$. Pick $1 \leq a_1 < a_2 < \cdots < a_k \leq n$ to form a set $\{a_1, a_2, \ldots, a_k\}$. Denote by M the product of the k integers. The set is called *good* if $a_i^2 \nmid M$ for all $i = 1, 2, \ldots, k$.

Let $h(n)$ be the size of the largest good set that can be formed.

(a) (3 points) Compute $h(6)$.

(b) (12 points) Determine $h(n)$. Partial credit will be awarded for finding good upper/lower bounds on $h(n)$.

The End