CUHK Department of Mathematics

Enrichment Programme for Young Mathematics Talents 2019

Number Theory and Cryptography (SAYT1114)

Quiz 1

- The total score for the quiz is $100 + 20$ (20 points for the bonus question).
- If you obtain X points, your score will be $\min(X, 100)$.
- Time allowed: $(60 + \varepsilon)$ minutes.
- The use of calculator is allowed.
- Unless otherwise specified, all variables defined in the quiz paper are integers.

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) Given a, b where $b > 0$. Then there exists a unique pair of integers (q, r) such that $a = qb + r$ and $0 < r \leq b$.

(b) (2 points) Given a, b, c where $c \neq 0$. If $c \nmid a + b$, then $c \nmid a$ and $c \nmid b$.

(c) (2 points) Let $a, b \neq 0$. If $a \mid b$ and $b \mid a$, then $a = b$.

(d) (2 points) $gcd(a, 1 - a^2) = 1$ for all integers a.

(e) (2 points) Given $a, b, c > 0$ such that $c = a + b$. Then $gcd(a, c) = gcd(b, c)$.

Q2. (10 points) Fill in the blanks to complete the following definitions and theorem statements. Each blank is worth 2 points.

(Definition of Divisibility) Let a and b be integers, $a \neq 0$. We say a divides b if there exists ____(a)____. In this case we write $a \mid b$.

(Bézout's Identity) Let m and n be integers, not both zero. Then there exists integers x and y such that ____(b)____ $= gcd(m, n)$.

(Euclid's Lemma) Let a, b, c be integers, $a \neq 0$. If $a \mid bc$ and ____(c)____, then $a \mid b$.

(Fundamental Theorem of Arithmetic) Given integer $n > 1$. Then we can write $n = p_1 \dots p_r$, where each p_i is a/an ____(d)____. Furthermore, the expression is ____(e)____.

Q3. **(30 points)** Let $a := 3990$ and $b := 728$.

(a) (10 points) Let $g := gcd(a, b)$. Using the Euclidean algorithm, find g.

(b) (10 points) Using the calculation in (a), find **one** solution to the linear Diophantine equation $3990x + 728y = g$.

(c) (10 points) Hence, find **all** solutions to the following linear Diophantine equations.

(i) (5 points) $3990x + 728y = 56$

(ii) (5 points) $3990x + 728y = 104$

Q4. **(25 points)** Prove the following statements. If you use the Fundamental Theorem of Arithmetic, at most 60% of the points will be awarded.

(a) (5 points) Given a, b, c, d with $a, b \neq 0$. Suppose $a \mid c$ and $b \mid d$. Then $ab \mid cd$.

(b) (10 points) Given a, b, c, all nonzero. Then $lcm(lcm(a, b), c) = lcm(a, lcm(b, c))$.

(c) (10 points) Given a, b, c, d, all nonzero. Then $gcd(a, c)gcd(b, d) \mid gcd(ab, cd)$.

Q5. **(25 points)** Given positive integers n and m, such that n is a perfect square, $m \mid n$, and m is square-free (that is, $a^2 \nmid m$ for all $a > 1$).

By the Fundamental Theorem of Arithmetic, we can find primes p_i and non-negative a_i and b_i $(1 \leq i \leq r)$, such that $n = p_1^{a_1} \dots p_r^{a_r}$ and $m = p_1^{b_1} \dots p_r^{b_r}$.

(a) (6 points) Translate the three given conditions into conditions on a_i and b_i.

(b) (8 points) Prove that $m^2 \mid n$. (Hint: prove that $a_i \geq 2b_i$ for each i.)

(c) (3 points) For each $k \geq 3$, find a counter-example to the following statement: Given positive integers n and m, such that n is a perfect k-th power, $m \mid n$, and m is k-th power-free (that is, $a^k \nmid m$ for all $a > 1$). Then $m^k \mid n$.

(d) (8 points) Prove the following "correct" generalization: Given positive integers n and m, such that n is a perfect k-th power, $m \mid n$, and m is square-free (that is, $a^2 \nmid m$ for all $a > 1$). Then $m^k \mid n$.

Q6 (Bonus Question). (20 points) Given $a, b > 0$ where $gcd(a, b) = 1$. For $c \geq 0$, we are interested in the existence of non-negative integer solutions to $ax + by = c$.

(a) (5 points) Consider an example: $a := 5, b := 7$. Copy the following table to your answer book. Circle all values of c for which $5x + 7y = c$ has **no** non-negative integer solutions.

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

(b) (15 points) Prove the following statements. Partial credit will be awarded for stating "meaningful" observations from part (a).

(i) (9 points) If $c \geq (a-1)(b-1)$, then $ax + by = c$ has non-negative integer solution.

(ii) (6 points) There are exactly $\frac{(a-1)(b-1)}{2}$ values of c for which $ax + by = c$ has no non-negative integer solutions.

The End