Assignment 3 Rubrics (100 points max, 110 points in total)

Q1 (5 points)

By definition, $ac|bc$ implies that there exists an integer k such that $bc = ack$. Divide c on both sides and we get $b = ak$. Again, by definition, this shows $a|b$.

- exist k (an interger), without (or with incorrect) this statement or some statement the same as this (**minus 1 point**)
- $ac|bc$ implies $bc = ack$(incorrect statement $kbc = ac$, **minus 1 point**)
- not prove by definition(**minus 2 points**)
- unreasonable proof(**minus 5 points**)

Q2 (5 points)

- (a) correct answer (**1 point**)
- (b) and (c) correct answer (**2 point**); only process correct but answer incorrect (**1 point**); only incorrect answer or both process and answer are incorrct (**0 point**).

Q3 (10 points)

- (a) and (b) correct answer (**2 point**); only process correct but answer incorrect (**1 point**); only incorrect answer or both process and answer are incorrct (**0 point**).
- (c) and (d) correct answer (**3 point**); only process correct but answer incorrect (**2 point**); only part of the process correct but answer incorrect (**1 point**); only incorrect answer or both process and answer are incorrct (**0 point**).

Q4 (5 points)

1. (2points) 1 point for process, 1 point for conclusion
2. (3points) 2 points for process, i point for conclusion

Q5 (20 points)

1. (5 points) 4 points for process, 1 point for conclusion
2. (5 points) 4 points for process, 1 point for conclusion
3. (2 points) only give x = certain concrete value -1
4. (8 points) 6 points for process, 2 points for conclusion (note: the problem ask the express of gcd(252,356) instead of gcd(267,79))

Q6 (5 points)

- gcd(b,c) = sb + sc (2 points)
- asb = skc (2 points)
- a * gcd(b,c) = (sk + at) * c (1 point)

Q7 (10 points)

a)

- ab ≡ 1 (mod m), ac ≡ 1 (mod m) (1 point)
- m | a(b - c) (2 points)
- m | (b - c) (1 point)
- b ≡ c (mod m) (1 point)

b)

- prove by contrapositive (1 point)
- aa' = 1 = km for some k (1 point)
- d | a and d | m (1 point)
- d | (aa' - km), d | 1 (1 point)
- d = 1 (1 point)

Q8 (10 points)

(a) Total score: 7 points.

- **(1) 2 points.** Proof that $\gcd(m_1, m_2, \ldots, m_k) = 1$
- **(2) 1 point.** Transformation of $a \equiv b (\bmod m_1)$ to $m_1 | (a - b)$ or other equivalent forms (such as $a - b = m_1 k_1$)
- **(3) 2 points.** Correctly deducing $a \equiv b (\bmod m_1 m_2)$ from $a \equiv b (\bmod m_1)$, $a \equiv b (\bmod m_2)$, and $\gcd(m_1, m_2) = 1$
- **(4) 2 points.** Generalizing (3) using (1) to the case $a \equiv b (\bmod m_1 m_2 \ldots m_k)$

(b) Total score: 3 points.

- **(1) 1 point.** Elaboration of the uniqueness definition of the Chinese Remainder Theorem: Unique under the product of moduli
- **(2) 1 point.** Proof by contradiction, assuming the existence of two different solutions under the product of moduli
- **(3) 1 point.** Using (a) to deduce their congruence, leading to a contradiction due to the product of moduli, thus proving the original proposition

Hint:

- Reasonable methods are scored accordingly, and points may be deducted for missing steps in the process.

Q9 (10 points)

(a) Total score: 5 points.

- **(1) 1 point.** $6 = 2 \times 3$, $10 = 2 \times 5$, $35 = 5 \times 7$
- **(2) 1 - 2 point.** Obtaining $x \equiv 5 (\bmod 6)$ and deriving $x \equiv 5 \equiv 1 (\bmod 2)$ and $x \equiv 5 \equiv 2 (\bmod 3)$
- **(3) 1 - 2 point.** Obtaining $x \equiv 3 (\bmod 10)$ and deriving $x \equiv 3 \equiv 1 (\bmod 2)$ and
- **(4) 1 - 2 point.** Obtaining $x \equiv 8 (\bmod 35)$ and deriving $x \equiv 8 \equiv 3 (\bmod 5)$ and

  *Note: (2), (3), (4) - Correctly writing one awards **2 points**, writing two awards **3 points**, writing all three awards **4 points**.*

(b) Total score: 5 points.

- **(1) 1 point.** $m = 2 \times 3 \times 5 \times 7 = 210$
- **(2) 1 point.** $M_1 = 105, M_2 = 70, M_3 = 70, M_3 = 42, M_4 = 30$
- **(3) 1 point** $y_1 = 1, y_2 = 1, y_3 = 3, y_4 = 4$
- **(4) 2 points** $x = 113 (\bmod 210)$ (**1 point** if only one correct special solution is provided).

Hint:

- Reasonable methods are scored accordingly, and points may be deducted for missing steps in the process.

Q10 (15 points)

The subtask is dependent, that means you can get the answer of task 4 even your prove is wrong in task 5.

(You can use other method.)

a

For this prove, you need to show the following steps, each step values 1 point.

You need to give the reason of every step unless the step is gotten from last step.

1. i · a ≡ j · a (mod p)
2. by definition p | (j − i)a
3. Since p is a prime and 1 ≤ j − i < p, we have gcd(p, j − i) = 1
4. hence p | a
5. contradicts the premise that a is not divisible by p

b

For this prove, you need to show the following steps, each step values 1 point.

You need to give the reason of every step unless the step is gotten from last step.

1. t p ł k ·a for k = 1, 2, . . . , p−1
2. {1 · a mod p, 2 · a mod p, . . . ,(p − 1)a mod p} = {1, 2, ..., p − 1}
3. none of the p − 1 integers in the left set is divisible by p

4. from (a) we know these $p - 1$ integers are distinct from each other when modulo p
5. multiplying all integers in each set results in the congruence: $a^{p-1} (p - 1)! \equiv (p - 1)! \pmod p$

C

For this prove, you need to show the following steps, previous two steps values 1 points, while the last values point.

You need to give the reason of every step unless the step is gotten from last step.

1. Since p is prime and $p \nmid (p - 1)!$, it follows that $\gcd(p,(p - 1)!) = 1$.
2. by definition, (b) shows that $p \mid (a^{p-1} - 1)(p - 1)!$.
3. $p \mid (a^{p-1} - 1)$, i.e., $a^{p-1} \equiv 1 \pmod p$

D

For this prove, you need to show the following steps, if all the two are true, get 2 points.

You need to give the reason of every step unless the step is gotten from last step.

1. If a is not divisible by p -> $a^p \equiv a \pmod p$
2. If a is divisible by p -> $a \equiv 0 \pmod p$ and hence $a^p \equiv 0 \pmod p$

(Someone lost one condition)

Q11 (5 points)

(a) (2 points)

1. Two points will be given for the correct process and answers
2. The process is correct (or point out **5^6 ≡ 1 (mod 7)**) ., but the final result is miscalculated, give one point
3. If the final answer is correct, but **you don't use Fermat's little theorem or you use it incorrectly**, you will be given one point

(b) (3 points)

1. Three points will be given for the correct process and answers
2. The process is correct (or point out **φ (15) = 8** or point out **a^8 ≡ 1 (mod 15)**), but the final result is miscalculated, one point is given
3. If you get **8^7 mod 15** or something like this and then calculate incorrectly, two points are given
4. If the final answer is correct, and **you don't use Euler's theorem or you use it incorrectly**, one point is given

Q12 (10 points)

(a) (3 points)

1. Three points will be given for the correct process and answers
2. If the final answer is incorrect, point out **C = M^e mod n** to give one point and substitute to get **8^7 mod 65** gives other one point.

(b) (4 points)

1. Four points are given for the correct process and answers
2. If the final answer is incorrect, point out **$\varphi(65) = 48$** to give one point and get **$7d \equiv 1 \pmod{48}$** gives other one point.

(c) (3 points)

1. Exactly right to give three points
2. If the final answer is incorrect, list **C^d mod n** to give one point and substitute to get **57^7 mod 65** gives other one point.

Contact

If you have any questions, contact corresponding TAs:

Q1-3 12332414 李昊洋

Q4-5 12111842 张羽乐

Q6-7 12111046 张天舒

Q8-9 12112910 罗嘉诚

Q10 12110416 刘家宝

Q11-12 12110411 伍福临

Grading: 12332414 李昊洋