ITCS 531: Number Theory 2 solutions

Rob Egrot

Q1

Suppose $x \equiv_n y$, and suppose $m|n$. Show that $x \equiv_m y$.

- Suppose $x - y = kn$, and $n = am$.
- Then $x - y = (ka)m$.

Q2

Complete the proof of proposition 2.8(2) (if $x \equiv_n x'$ and $y \equiv_n y'$ then $xy \equiv_n x'y'$).

- Suppose $(x - x') = kn$ and $(y - y') = ln$.

$$\begin{aligned} xy - x'y' &= xy - xy' + xy' - x'y' \\ &= x(y - y') - y'(x - x') \\ &= xln - y'kn \\ &= (xl - y'k)n. \end{aligned}$$

Q3

Calculate $2^{2^{13543}} \mod 3$.

- $2 \equiv_3 -1$, and 2^{13543} is an even number.
- -1 to the power of any even number is 1.
- So $2^{2^{13543}} \equiv_3 1$.

Q4

Let p and q be distinct primes, and let $x \in \mathbb{Z}$. Prove that if $p|x$ and $q|x$, then $pq|x$.

- We know $x = (\pm 1)p_1 \dots p_n$ for some primes $p_1, \dots, p_n$.
- Also, since $p|p_1 \dots p_n$ we must have $p = p_i$ for some i.
- We also have $q|x$, and so $q = p_j$ for some j.
- Since p and q are distinct, we can't have $i = j$.
- Assume without loss of generality that $i = 1$ and $j = 2$.
- Then $x = (\pm 1)(pq)p_3 \dots p_n$.
- So $pq|x$.

Q5

a) Prove that $4 = 9 = -1 \mod 5$.

b) Prove that $4^{1536} \equiv_7 9^{4824}$ (HINT: $9 \equiv_7 2$ and $8 \equiv_7 1$).

c) Prove that $4^{1536} \equiv_{35} 9^{4824}$.

Q5, a) and b)

a) Prove that $4 = 9 = -1 \mod 5$.

- $4 - (-1) = 5$, and $9 - (-1) = 2(5)$.

b) Prove that $4^{1536} \equiv_7 9^{4824}$

$$\begin{aligned} 4^{1536} &= 2^{2(1536)} \\ &= 2^{3072} \\ &= 2^{3(1024)} \\ &= 8^{1024} \\ &\equiv_7 1^{1024} \\ &\equiv_7 1. \end{aligned}$$

$$\begin{aligned} 9^{4824} &\equiv_7 2^{4824} \\ &= 2^{3(1608)} \\ &= 8^{1608} \\ &\equiv_7 1^{1608} \\ &\equiv_7 1. \end{aligned}$$

Q5, c)

c) Prove that $4^{1536} \equiv_{35} 9^{4824}$.

- From part a):
  - $4^{1536} \equiv_5 (-1)^{1536} \equiv_5 1$.
  - $9^{4824} \equiv_5 (-1)^{4824} \equiv_5 1$.
- This means $4^{1536} \equiv_5 9^{4824}$.
- So $5 | (4^{1536} - 9^{4824})$.
- In part b) we proved that $4^{1536} \equiv_7 9^{4824}$.
- So $7 | (4^{1536} - 9^{4824})$.
- By Q4 this means $35 | (4^{1536} - 9^{4824})$.
- I.e. $4^{1536} \equiv_{35} 9^{4824}$.

Q6

Let X be a set and let $\{Y_i : i \in I\}$ be a partition of X. Prove that the binary relation R, defined by $R(x, y) \iff x$ and y are in Y_i for some $i \in I$, is an equivalence relation.

- R is reflexive:
  - $R(x, x)$ because x is always in the same part of the partition as itself.
- R is symmetric:
  - Suppose $R(x, y)$.
  - Then x and y are in the same part of the partition.
  - But then $R(y, x)$ by definition.
- R is transitive:
  - Suppose $R(x, y)$ and $R(y, z)$.
  - Then x is in the same part of the partition as y, and y is in the same part of the partition as z.
  - But this means x is in the same part of the partition as z.
  - So $R(x, z)$.

Q7

a) Prove that $R(x, y) \iff R_{P_R}(x, y)$ for all $x, y \in X$.

b) State and prove a similar conjecture on converting from partitions to equivalence relations and back to partitions.

- Proof for a):
- Suppose first that $R(x, y)$.
- Then $y \in [x]$.
- I.e. y and x are in the same part of the partition P_R.
- But this means $R_{P_R}(x, y)$.
- Conversely, if $R_{P_R}(x, y)$, then $y \in [x]$.
- I.e. $R(x, y)$.
- This shows $R = R_{P_R}$.

Q7, b)

b) State and prove a similar conjecture on converting from partitions to equivalence relations and back to partitions.

- The sensible conjecture is that $P_{R_P} = P$.
- To prove this, let $P = \{X_i : i \in I\}$.
- We want to show that $\{X_i : i \in I\} = \{[x]_{R_P} : x \in X\}$.
- First, given any $x \in X$ we must have $x \in X_i$ for some i, as P is a partition.
- We must prove that $[x]_{R_P} = X_i$.

$$\begin{aligned} y \in [x]_{R_P} &\iff R_P(x, y) \\ &\iff y \in X_i. \end{aligned}$$

- This proves the claim because, because every $[x]_{R_P}$ is equal to X_i where $x \in X_i$, and every X_i is equal to $[x]_{R_P}$ for $x \in X_i$.