Lecture 20

Enoch Cheung

November 7, 2013

1. Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. If $\gcd(a, m) = 1$ then a^{-1} is unique modulo m.

   Suppose $\gcd(a, m) = 1$ with $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$ (so b and c are both multiplicative inverses of a). Then because multiplication is commutative $ac \equiv 1 \pmod{m}$. Therefore,

   $$ba \equiv 1 \pmod{m} \implies bac \equiv c \pmod{m} \implies b(ac) \equiv c \pmod{m} \implies b \equiv c \pmod{m}$$

   Therefore, $b \equiv c \pmod{m}$ so a^{-1} is unique modulo m.

2. **Lemma.** If $n \in \mathbb{N}$ and $a_1, a_2, \ldots, a_n \in \mathbb{N}$ and $p|(a_1 a_2 \cdots a_n)$ then $\exists i \in \mathbb{N}$ with $1 \leq i \leq n$ such that $p|a_i$.

   Note that this is only true for prime p.

   We prove this by induction on n. Base case: If $p|a_1$ then $p|a_1$.

   Inductive case: Assume that for any $a_1, \ldots, a_n \in \mathbb{N}$, $p|(a_1 a_2 \cdots a_n)$ implies $p|a_i$ for some $1 \leq i \leq n$.

   Now given $a_1, \ldots, a_n, a_{n+1} \in \mathbb{N}$, then if $p|a_{n+1}$ then we are done. Otherwise, $p \nmid a_{n+1}$, and since p is prime, this means that p, a_{n+1} are relatively prime. By Euclid's Lemma (Lemma 6.5.25), since $p|(a_1 \cdots a_n \cdot a_{n+1})$ and p, a_{n+1} are relatively prime, so $p|(a_1 \cdots a_n)$. Therefore, by inductive hypothesis, $p|a_i$ for some $1 \leq i \leq n$.

3. (a) $6x \equiv 1 \pmod{13}$.

   Note that $6 \cdot 2 \equiv 12 \equiv -1 \pmod{13}$, so $6(-2) \equiv 1 \pmod{13}$. Therefore, $x \equiv -1 \pmod{13}$. By question 1, multiplicative inverses are unique so -2 is the only solution modulo m.

   (b) $4x + 3 \equiv 1 \pmod{9}$.

   Note that $4 \cdot (-2) \equiv 1 \pmod{9}$. Therefore,

   $$4x+3 \equiv 1 \pmod{9} \iff 4x \equiv -2 \pmod{9} \iff x \equiv (-2)(-2) \pmod{9} \iff x \equiv 4 \pmod{9}$$

   (c) $6x - 4 \equiv 12 \pmod{15}$

   There are no such solutions x, because $6, 15$ are not relatively prime, so 6 has no inverse modulo 15.

   Suppose $6x - 4 \equiv 12 \pmod{15}$ for some x, then $6x \equiv 16 \equiv 1 \pmod{15}$, so x is the multiplicative inverse to 6, which does not exist.

4. Let $a, b \in \mathbb{Z}$ and $m, d \in \mathbb{N}$. Assume $d = \gcd(a, m)$. Consider the linear congruence $ax \equiv b \pmod{m}$.

   (a) If $d \nmid b$, can there be any $x \in \mathbb{Z}$ satisfying this congruence?

   No. Suppose $ax \equiv b \pmod{m}$ for some x, then $m|(b - ax)$. Since $d|m$, this means that $d|(b - ax)$. Note that $d|a$ so $d|ax$. Therefore, $d|b$ which is a contradiction.

   (b) If $d|b$ why can we say that there are solutions to this congruence?

   Since $d = \gcd(a, m)$ there are $s, t \in \mathbb{N}$ such that $as + mt = d$, so taken mod m, this means that $as \equiv d \pmod{m}$ (s is something similar to an inverse of a, but instead of 1 it gives d because a need not have an inverse if $d > 1$). This s need not be unique modulo m.

   Suppose $a = cd$, then c, m are relatively prime, since if $\ell|c$ and $\ell|m$, then $\ell d|a$ and $\ell d|m$ so d would not be the gcd. Therefore, c^{-1} exists mod m, so

   $$ax \equiv b \pmod{m} \iff cdx \equiv b \pmod{m} \iff xd \equiv c^{-1}b \pmod{m}$$

   so we can let $c^{-1}b = yd$ then we are looking for solutions of $xd \equiv yd \pmod{m}$ where $d|m$.

   Lemma. If $d|m$ then

   $$xd \equiv yd \pmod{m} \iff x \equiv y \pmod{\frac{m}{d}}$$

Proof: Certainly, if $x \equiv y \pmod{\frac{m}{d}}$, then $\frac{m}{d}|(x-y)$ so $m|(x-y)$. Now suppose $xd \equiv yd \pmod{m}$, then $m|(xd-yd)$ so $mk = (x-y)d$ for some $k \in \mathbb{N}$. Therefore, $\frac{m}{d}k = x - y$ so $\frac{m}{d}|(x-y)$. □

Therefore, since $d|b$, using the lemma,

$$ax \equiv b \pmod{m} \iff xd \equiv c^{-1}b \pmod{m} \iff x \equiv c^{-1}\frac{b}{d} \pmod{\frac{m}{d}}$$

so there are d solutions modulo m, since if $x \equiv t \pmod{\frac{m}{d}}$ is a solution, then $t, t+\frac{m}{d}, t+\frac{2m}{d}, \ldots, t+\frac{(d-1)m}{d}$ are all solutions distinct mod m.

(c) $9x \equiv 12 \pmod{15}$.

Note that $9 \cdot 2 \equiv 18 \equiv 3 \pmod{15}$, so $9 \cdot 2 \cdot 4 \equiv 12 \pmod{15}$. Therefore, $x \equiv 8 \pmod{15}$ is a solution. Since $\gcd(9, 15) = 3$, there are 3 solutions, and we have shown that $8, 8+5, 8+2\cdot 5$ are all solutions, so $x \equiv 8, 13, 3$ are all distinct solutions mod 15.

5. Let $a, b, c \in \mathbb{Z}$. Prove that $\gcd(a, b) = \gcd(a + cb, b)$.

We wish to show that the set of common divisors of a, b and $(a+cb), b$ are the same.

Suppose d is a common divisor of a, b, then $d|a$ and $d|b$, so $d|cb$, so $d|(a+cb)$. Therefore, d is a common divisor of $(a+cb), b$.

Now suppose d is a common divisor of $(a+cb), b$, then $d|(a+cb)$ and $d|b$. So $d|-cb$, so $d|(a+cb-cb)$ so $d|a$. Therefore, d is a common divisor of a, b.