15-151 Midterm 2 Review

Eric Zheng

October 22, 2019

1 Named Theorems and Important Results

Theorem 1.1: Bezout's lemma

For all $a, b, c \in \mathbb{Z}$, the equation $ax + by = c$ has a solution $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$.

Proof. We will prove the bi-implication in each direction separately.

- ($\Longrightarrow$) Suppose $\exists x, y \in \mathbb{Z}$ such that $ax + by = c$. By definition, $\gcd(a, b)$ must divide both a and b, so we can write:

  $$n \cdot \gcd(a, b) = a \qquad m \cdot \gcd(a, b) = b$$

  for some $n, m \in \mathbb{Z}$. So we have:

  $$\begin{aligned} c &= ax + by \\ &= nx \cdot \gcd(a, b) + my \cdot \gcd(a, b) \\ &= (nx + my) \cdot \gcd(a, b) \end{aligned}$$

  Then $\gcd(a, b) \mid c$, as required.

- ($\Longleftarrow$) We will prove this for $a, b \in \mathbb{N}$. Since $x, y \in \mathbb{Z}$, the result holds in general. Consider the following predicate:

  $p(n) :=$ "if $a + b = n$ and $\gcd(a, b) \mid c$, then $\exists x, y \in \mathbb{Z}$ such that $ax + by = c$"

  We proceed by induction on $n = a + b$.

  - *Base case.* If $n = 0$, then $a = b = 0$, so $\gcd(a, b) = 0$. Now if $0 \mid c$, then $c = 0$. Any $x, y \in \mathbb{Z}$ will satisfy $ax + by = c$.
  - *Induction step.* Let $n \geq 0$ be given, and assume that $p(k)$ holds for all $k \leq n$. Let $a, b \in \mathbb{N}$ such that $a + b = n + 1$, and suppose $c \in \mathbb{Z}$ such that $\gcd(a, b) \mid c$. Then there are three cases:
    1. Case $a = b = 0$. This case is not possible, since $n + 1 > 0$.

2. Case one of a or b is zero. Without loss of generality, let $a = 0$. Then $\gcd(a, b) = b$, so by the induction hypothesis, $b \mid c$. By definition, $\exists y \in \mathbb{Z}$ such that $by = c$.
3. Case $a, b > 0$. Without loss of generality, let $b \geq a$. Note that $a + (b - a) = b$, and $b \in [n]$. Additionally, since $\gcd(a, b - a) = \gcd(a, b)$, we have $\gcd(a, b - a) \mid c$. Now since $p(b)$ is true, there must exist some $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + (b - a)y_0 = c$. But this implies that $a(x_0 - y_0) + by_0 = c$, so we have found a solution to $ax + by = c$.

□

Theorem 1.2: coprime (Euclid's) lemma

For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$, then $a \mid bc$ implies that $a \mid c$.

Proof. Let $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. Now suppose that $a \mid bc$. By Bezout's lemma (Theorem 1.1), $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. This implies that $cax + cby = c$. Clearly, $a \mid cax$, and by our assumption, $a \mid cby$. Thus, a divides their sum, or $a \mid c$, as required. □

Theorem 1.3: solutions to linear Diophantine equations

For all $a, b, c \in \mathbb{Z}$, if $x_0, y_0 \in \mathbb{Z}$ satisfy $ax_0 + by_0 = c$, then for some $x, y \in \mathbb{Z}$, $ax + by = c$ if and only if x and y are of the form:

$$x = x_0 + \frac{b}{\gcd(a, b)} \cdot k \qquad y = y_0 - \frac{a}{\gcd(a, b)} \cdot k$$

for some $k \in \mathbb{Z}$. (We have implicitly assumed that $\gcd(a, b) \neq 0$, which is true if at least one of a and b is nonzero.)

Proof. We will prove each direction of the bi-implication separately.

- ($\Longrightarrow$) Suppose $x_0, y_0 \in \mathbb{Z}$ satisfy $ax_0 + by_0 = c$. Now consider another pair $x, y \in \mathbb{Z}$ which also satisfy $ax + by = c$. Now note:

$$\begin{aligned} & ax + by = c = ax_0 + by_0 \\ \Longrightarrow\ & a(x - x_0) = b(y_0 - y) \\ \Longrightarrow\ & \frac{a}{\gcd(a, b)}(x - x_0) = \frac{b}{\gcd(a, b)}(y_0 - y) \end{aligned}$$

Thus, we have:

$$\frac{a}{\gcd(a,b)} \mid \frac{b}{\gcd(a,b)}(y_0 - y)$$
$$\frac{b}{\gcd(a,b)} \mid \frac{a}{\gcd(a,b)}(x - x_0)$$

But observe that:

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

So by Euclid's lemma (Theorem 1.2), we must have:

$$\frac{a}{\gcd(a,b)} \mid (y_0 - y) \implies y = y_0 - \frac{a}{\gcd(a,b)} \cdot k$$
$$\frac{b}{\gcd(a,b)} \mid (x - x_0) \implies x = x_0 + \frac{b}{\gcd(a,b)} \cdot k$$

for some $k \in \mathbb{Z}$. (It technically remains to be shown that the k in the expressions for x and y are the same, but this is easy to do by contradiction.)

- ($\Longleftarrow$) Let $x_0, y_0 \in \mathbb{Z}$ satisfy $ax_0 + by_0 = c$, and consider some arbitrary x, y of the form:

$$x = x_0 + \frac{b}{\gcd(a,b)} \cdot k$$
$$y = y_0 - \frac{a}{\gcd(a,b)} \cdot k$$

for some $k \in \mathbb{Z}$. Now consider the linear combination $ax + by$:

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{\gcd(a,b)} \cdot k\right) + b\left(y_0 - \frac{a}{\gcd(a,b)} \cdot k\right) \\ &= ax_0 + by_0 + \frac{abk}{\gcd(a,b)} - \frac{abk}{\gcd(a,b)} \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

$\square$

Theorem 1.4: Wilson's theorem

If $p \in \mathbb{N}$ is prime, then $(p-1)! \equiv -1 \bmod p$.

Proof. Observe that:

$$(p-1)! = (p-1)(p-2)(p-3)\dots(3)(2)(1)$$

Since $(p-1)(1) \equiv -1 \bmod p$, it suffices to show instead that

$$(p-2)(p-3)\dots(3)(2) \equiv 1 \bmod p$$

First, we note that since each term $a_k = (p-k)$ in this product is coprime with p, by Bezout's lemma (Theorem 1.1) it must have some multiplicative inverse among the factors. That is, there must be an integer solution to $a_k x + py = 1$ for all $2 \leq k \leq p-2$. By definition, we have $a_k x \equiv 1 \bmod p$, so x is the multiplicative inverse of the term a_k. Under modular arithmetic, we can take $0 \leq x < p-1$, yet x cannot be 0, 1, or $p-1$. Thus, every term a_k has a multiplicative inverse that is another term a_i.

Next, we show that no term a_k is its own inverse. If we had $a_k^2 \equiv 1 \bmod p$, then $a_k^2 - 1 \equiv (a_k+1)(a_k-1) \equiv 0 \bmod p$. Since p is prime, this implies that $a_k \equiv \pm 1 \bmod p$. (This was a homework exercise!) But $a_k \not\equiv \pm 1 \bmod p$ if we take k between 2 and $p-2$, so the inverse of each a_k must be distinct from a_k itself.

From these two results, it follows that we can pair each term a_k with its multiplicative inverse, so the resulting product must be 1, as required. □

Theorem 1.5: Fermat's little theorem

If $p \in \mathbb{N}$ is prime, then for all $a \in \mathbb{Z}$, $a^p \equiv a \bmod p$. If we additionally have $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \bmod p$.

Proof. We will prove the second version of this theorem (which requires that $\gcd(a,p) = 1$). Let $p \in \mathbb{N}$ be prime, and denote $S = \{a, 2a, \dots, (p-1)a\}$. We note two things:

1. No distinct $x, y \in S$ satisfy $x \equiv y \bmod p$. To show this, assume for the sake of contradiction that $ma \equiv na \bmod p$ for some $m, n \in [p-1]$, yet $m \neq n$. Then $p \mid a(m-n)$, so we must have $p \mid a$ or $p \mid m-n$ since p is prime. But $\gcd(a,p) = 1$, so $p \nmid a$, and $m - n \in [p-1]$, so $p \nmid m-n$ by irreducibility. This is a contradiction, so our assumption is false.

2. For each $x \in S$, $\exists y \in [p-1]$ such that $x \equiv y \bmod p$. We note that, under modulus p, each $x \in S$ must be congruent to some $0 \leq y < p$. But observe that $y \neq 0$, since otherwise, it would follow that $p \mid x$. Again, this is not possible by the irreducibility of p (see Theorem 2.1).

Now consider the product $a^{p-1}(p-1)!$ of all the elements in S. As we have shown, each distinct $x \in S$ is congruent to some distinct $y \in [p-1]$, so the elements are congruent to a permutation of $[p-1]$. It follows that:

$$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$$

And since, by Bezout's lemma (Theorem 1.1), each $y \in [p-1]$ has some multiplicative inverse, this is equivalent to saying:

$$a^{p-1} \equiv 1 \bmod p$$

as required. $\square$

Theorem 1.6: Euler's theorem

For all $a \in \mathbb{Z}$, $n \in \mathbb{N}$, if $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Remark. Note that Fermat's little theorem (Theorem 1.5) is a special case of Euler's theorem (Theorem 1.6). Euler's theorem will not be on the exam, but it can't hurt to know it.

2 Other Interesting Results from Class

Theorem 2.1: equivalence of primality and irreducibility

An integer p is prime if and only if it is irreducible.

Proof. We will prove each direction of the bi-implication separately.

- ($\Longrightarrow$) Let $p \in \mathbb{Z}$ be a prime number. Now suppose we can express p as $p = ab$ for some $a, b \in \mathbb{Z}$. Then $p \mid ab$, so by definition, $p \mid a$ or $p \mid b$. Without loss of generality, let $p \mid a$. Now $pq = a$ for some $q \in \mathbb{Z}$, so $p = ab \implies p = pqb \implies 1 = qb$. It follows that b must be a unit, so p is irreducible.

- ($\Longleftarrow$) Let $p \in \mathbb{Z}$ be irreducible, and suppose that $p \mid ab$. Now there are two cases:

  - Case $p \mid a$. In this case, p is prime by definition.
  - Case $p \nmid a$. In this case, note that, by irreducibility, the only factors of p are $\{\pm 1, \pm p\}$. Since $p \neq a$ (otherwise, $p \mid a$), we must have $\gcd(p, a) = 1$. Then by Euclid's lemma (Theorem 1.2), we must have $p \mid b$, so p is prime by definition.

$\square$

Theorem 2.2: existence of prime factorization

For all $n \in \mathbb{N}$ such that $n \geq 2$, n can be factored into the product of prime numbers.

Proof. Let $p(n) :=$ "n can be factored into the product of prime numbers". We will proceed by strong induction on n.

- *Base case.* Consider $n = 2$. Since 2 is prime, $p(2)$ holds.
- *Induction step.* Let $n \geq 2$ be given, and assume that $p(k)$ holds for all $2 \leq k \leq n$. Now consider $n + 1$. There are two possibilities:
  1. Case $n + 1$ is prime. Then $p(n + 1)$ is true.
  2. Case $n + 1$ is not prime. Then we can write $n + 1 = ab$ for some non-unit, non-zero $a, b \in \mathbb{N}$. But since $2 \leq a, b \leq n$, we know that a and b factor into primes by invoking the induction hypothesis. Thus, $n + 1 = ab$ must factor into primes.

$\square$

Theorem 2.3: uniqueness of prime factorization

For all $n \in \mathbb{N}$ such that $n \geq 2$, n can be uniquely factored into the product of prime numbers.

Proof. Consider the predicate:

$$p(n) := \text{“}n \text{ can be factored uniquely into the product of primes”}$$

We proceed by strong induction on $n \geq 2$.

- *Base case.* Let $n = 2$. There is only one way to factor 2 into primes, namely $p_1 = q_1 = 2$. Thus, $p(2)$ holds.
- *Induction step.* Let $n \geq 2$ be given, and assume that $p(i)$ holds for all $2 \leq i \leq n$. Consider two prime factorizations written in non-decreasing order:

  $$\begin{aligned} n + 1 &= p_1 \cdot p_2 \cdot p_3 \cdots p_k \\ &= q_1 \cdot q_2 \cdot q_3 \cdots q_l \end{aligned}$$

  Without loss of generality, let $p_1 \leq q_1$. Now since p_1 is prime and divides $q_1 \cdot q_2 \cdots q_l$, we must have $p_1 = q_i$ for some $i \in [l]$. But since the q's are in non-decreasing order, we must have $q_1 \leq q_i = p_1$. Since $p_1 \leq q_1 \leq p_1$, we must have $p_1 = q_1$. Then:

  $$p_2 \cdot p_3 \cdots p_k = q_2 \cdot q_3 \cdots q_l$$

  Now there are two possibilities:

  1. If there are no more prime factors, then we have shown $p(n + 1)$ to be true.

2. Otherwise, $2 \le p_2 \cdot p_3 \cdots p_k \le n$. In this case, we invoke the induction hypothesis to show that $p(n+1)$ is true.

$\square$

Theorem 2.4: divisibility tricks

Let $n \in \mathbb{N}$ have the base-ten expansion $d_0 d_1 d_2 \ldots d_r$. We claim:

1. $n \equiv \sum_{i=0}^{r} d_i \bmod 3$
2. $n \equiv \sum_{i=0}^{r} d_i \bmod 9$
3. $n \equiv \sum_{i=0}^{r} (-1)^i d_i \bmod 11$

Proof. Note that the decimal expansion satisfies:

$$n = \sum_{i=0}^{r} d_i 10^i$$

Now examining each trick:

1. Observe that $10 \equiv 1 \bmod 3$, so $10^k \equiv 1^k \equiv 1 \bmod 3$ for all $k \in \mathbb{N}$.
2. Observe that $10 \equiv 1 \bmod 9$, so $10^k \equiv 1^k \equiv 1 \bmod 9$ for all $k \in \mathbb{N}$.
3. Observe that $10 \equiv -1 \bmod 11$, so $10^k \equiv (-1)^k \bmod 11$ for all $k \in \mathbb{N}$.

$\square$

3 Eric's Personal Reminders

Here are a few things that I tend to forget easily:

1. Don't gloss over induction mechanics! In particular, remember to define the predicate as $p(n) :=$ "...". Also quantify stuff where appropriate.
2. Don't forget the exponent in Fermat's little theorem (Theorem 1.5) is $p-1$, **not** p. On a similar note, the theorem has the requirement that a and p be coprime.
3. Go over the divisibility tricks before the exam!