Math 3527 (Number Theory 1)

Lecture #23

Generalizing theorems in $\mathbb{Z}/m\mathbb{Z}$ to general Euclidean domains:

- The Chinese Remainder Theorem
- Euler's Theorem
- Fermat's Little Theorem

This material represents §4.2.4 and §4.2.5 from the course notes.

Chinese Remainder Theorem, Outline

Organization of the Chinese Remainder Theorem in $\mathbb{Z}/m\mathbb{Z}$:

- Solve a single linear congruence $ax \equiv b$ (mod m.
- Solve a system of congruences of the form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \vdots &\quad \vdots \quad \vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

Linear Congruences, I

We start by describing what to do with a single linear congruence:

Proposition (Linear Congruences)

Let R be a Euclidean domain, with $a, b \in R$, and let d any gcd of a and r. Then the equation $ax \equiv b \pmod{r}$ has a solution for $x \in R$ if and only if $d|b$. In this case, if $a = a'd$, $b = b'd$, and $r = r'd$, then $ax \equiv b \pmod{r}$ is equivalent to $a'x \equiv b' \pmod{r'}$ and the solution is $x \equiv (a')^{-1}b' \pmod{r'}$.

We can do all of these calculations using only the Euclidean algorithm.

Linear Congruences, II

The proof of the result is the same as over $\mathbb{Z}$.

- Proof: If x is a solution to the congruence $ax \equiv b \pmod{r}$, then there exists an $s \in R$ with $ax - rs = b$. Then since d divides the left-hand side, it must divide b.
- Now if we set $a' = a/d$, $b' = b/d$, and $r' = r/d$, our original equation becomes $a'dx \equiv b'd \pmod{r'd}$.
- Solving this equation is equivalent to solving $a'x \equiv b' \pmod{r'}$, by one of our properties of congruences.
- But since a' and r' are relatively prime, a' is a unit modulo r', so we can simply multiply by its inverse to obtain $x \equiv b' \cdot (a')^{-1} \pmod{r'}$.

Linear Congruences, III

Example: Solve $(7+i)x \equiv 3-i$ modulo $8-9i$ in $\mathbb{Z}[i]$.

Linear Congruences, III

Example: Solve $(7+i)x \equiv 3-i$ modulo $8-9i$ in $\mathbb{Z}[i]$.

- Using the Euclidean algorithm we can verify that $7+i$ and $8-9i$ are relatively prime, and can write 1 as a linear combination explicitly as

$$1 = (11-i)(7+i) + (-4-5i)(8-9i).$$

- So the inverse of $7+i$ modulo $8-9i$ is $11-i$.
- Now multiply both sides of the original congruence by $11-i$:

$$x \equiv (11-i)(7+i)x \equiv (11-i)(3-i) \equiv 3+i \pmod{8-9i}$$

and so the solution is $\boxed{x \equiv 3+i \pmod{8-9i}}$.

Linear Congruences, IV

Example: Solve $(x+1)p \equiv x^2+1$ modulo x^3+x+1 in $\mathbb{F}_3[x]$.

Linear Congruences, IV

Example: Solve $(x+1)p \equiv x^2+1$ modulo x^3+x+1 in $\mathbb{F}_3[x]$.

- Using the Euclidean algorithm we can verify that $x+1$ and x^3+x+1 are relatively prime, and can write 1 as a linear combination explicitly as

$$1 = (x^2+2x+2)(x+1) + 2(x^3+x+1)$$

- So the inverse of $x+1$ modulo x^3+x+1 is x^2+2x+2.
- Now multiply both sides of the original congruence by x^2+2x+2 and reduce:

$$p \equiv (x^2+2x+2)(x^2+1) \equiv 2x^2+2x \pmod{x^3+x+1}$$

and so the solution is $\boxed{p \equiv 2x^2+2x \pmod{x^3+x+1}}$.

Chinese Remainder Theorem, I

Now we can give the analogue of the Chinese Remainder Theorem:

Theorem (Chinese Remainder Theorem)

Let R be a Euclidean domain and $r_1, r_2, \dots, r_k$ be pairwise relatively prime elements of R, and $a_1, a_2, \dots, a_k$ be arbitrary elements of R. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{r_1} \\ x &\equiv a_2 \pmod{r_2} \\ \vdots & \quad \vdots \quad \vdots \\ x &\equiv a_k \pmod{r_k} \end{aligned}$$

has a solution $x_0 \in R$. Furthermore, x is unique modulo $r_1 r_2 \cdots r_k$, and the general solution is precisely the residue class of x_0 modulo $r_1 r_2 \cdots r_k$.

Chinese Remainder Theorem, II

The proof is the same as over $\mathbb{Z}$. By induction, it is enough to show the result for two congruences

$$\begin{aligned} x &\equiv a_1 \pmod{r_1} \\ x &\equiv a_2 \pmod{r_2}. \end{aligned}$$

Existence:

- The first congruence implies $x = a_1 + kr_1$ for some $k \in R$.
- Then plugging into the second equation then yields $a_1 + kr_1 \equiv a_2 \pmod{r_2}$.
- Rearranging yields $kr_1 \equiv (a_2 - a_1) \pmod{r_2}$.
- Since by hypothesis r_1 and r_2 are relatively prime, that this congruence has a unique solution for k modulo r_2, and hence has a solution for x.

Chinese Remainder Theorem, III

Uniqueness:

- Suppose x and y are both solutions, so that

$$\begin{aligned} x \equiv y &\equiv a_1 \pmod{r_1} \\ x \equiv y &\equiv a_2 \pmod{r_2}. \end{aligned}$$

- Then $x - y$ is congruent to 0 modulo r_1 and to 0 modulo r_2, meaning that $r_1 | (x - y)$ and $r_2 | (x - y)$.
- But since r_1 and r_2 are relatively prime, their product must therefore divide $x - y$, meaning that x is unique modulo $r_1 r_2$.
- Finally, it is obvious that any other element of R congruent to x modulo $r_1 r_2$ also satisfies the system.

We have shown both parts, so we are done.

Chinese Remainder Theorem, IV

Example: In $R = \mathbb{C}[x]$, solve the system $q(x) \equiv 1 \pmod{x-1}$, $q(x) \equiv 3 \pmod{x}$.

- Since $x - 1$ and x are relatively prime polynomials, by the Chinese Remainder Theorem we just need one solution.
- If we take the solution $q(x) = 3 + ax$ to equation 2 and plug it into equation 1, we must solve $3 + ax \equiv 1 \pmod{x-1}$.
- Since $3 + ax \equiv (3 + a) \bmod (x - 1)$, we can take $a = -2$.
- Hence the polynomial $q(x) = 3 - 2x$ is a solution.
- The general solution is therefore $\boxed{3 - 2x + x(x-1) \cdot s(x)}$ for an arbitrary polynomial $s(x) \in R$.
- Equivalently, the solution is $\boxed{q(x) \equiv 3 - 2x \pmod{x^2 - x}}$.

Euler and Fermat, I

Now we discuss the generalizations of Euler's and Fermat's theorems to R/pR. First, we need the general definition of the order of an element:

Definition

If R is a commutative ring with 1 and u is a unit of R, then the smallest $k > 0$ such that $u^k \equiv 1 \pmod{m}$ is called the order of u. (If there exists no such k, then we say u has infinite order.)

Examples:

- The element -1 has order 2 in $\mathbb{Z}$ (and also in $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$).
- The element i has order 4 in $\mathbb{Z}[i]$ and in $\mathbb{C}$.
- The element 2 does not have finite order in $\mathbb{R}$, since no positive power of 2 is equal to 1.

Euler and Fermat, II

Properties of Orders: Suppose R is a commutative ring with 1 and u is a unit in R. Then:

- If $u^n \equiv 1 \pmod{m}$ for some $n > 0$, then the order of u is finite and divides n.
- If u has order k, then u^n has order $k/\gcd(n,k)$. In particular, if n and k are relatively prime, then u^n also has order k.
- If $u^n \equiv 1 \pmod{m}$ and $u^{n/p} \not\equiv 1 \pmod{m}$ for any prime divisor p of n, then u has order n.
- If u has order k and w has order l, where k and l are relatively prime, then uw has order kl.

The proofs are the same as in $\mathbb{Z}/m\mathbb{Z}$.

Euler and Fermat, III

We can now give the generalization of Euler's theorem:

Theorem (Euler's Theorem)

If R is a commutative ring with 1 and $r \in R$, let $\varphi(r)$ denote the number of units in the ring R/rR, assuming this number is finite. Then if a is any unit in R/rR, we have $a^{\varphi(r)} \equiv 1 \pmod{r}$.

In fact, this result holds in any commutative ring S having a finite number of units. The idea of the proof is the same as over $\mathbb{Z}/m\mathbb{Z}$: the point is that if a is a unit and $u_1, \ldots, u_k$ are the units in S, then the elements $au_1, \ldots, au_k$ are the same as $u_1, \ldots, u_k$, just in a different order.

Euler and Fermat, IV

Proof:

- Let the set of all units in R/rR be $\overline{u_1}$, $\overline{u_2}$, ... , $\overline{u_{\varphi(r)}}$, and consider the elements $\overline{a \cdot u_1}, \overline{a \cdot u_2}, \dots, \overline{a \cdot u_{\varphi(r)}}$ in R/rR: we claim that they are simply the elements $\overline{u_1}$, $\overline{u_2}$, ... , $\overline{u_{\varphi(r)}}$ again (possibly in a different order).
- Since there are $\varphi(r)$ elements listed and they are all still units, it is enough to verify that they are all distinct.
- So suppose $a \cdot u_i \equiv a \cdot u_j \pmod{r}$. Since a is a unit, multiply by a^{-1}: this gives $u_i \equiv u_j \pmod{r}$, but this forces $i = j$.
- Hence modulo r, the elements $\overline{a \cdot u_1}, \overline{a \cdot u_2}, \dots, \overline{a \cdot u_{\varphi(r)}}$ are simply $\overline{u_1}$, $\overline{u_2}$, ... , $\overline{u_{\varphi(r)}}$ in some order.
- Thus $(a \cdot u_1)(a \cdot u_2) \cdots (a \cdot u_{\varphi(r)}) \equiv u_1 \cdot u_2 \cdots u_{\varphi(r)} \pmod{r}$ and so cancelling $u_1 \cdot u_2 \cdots u_{\varphi(r)}$ from both sides yields $a^{\varphi(r)} \equiv 1 \pmod{r}$ as desired.

Euler and Fermat, V

<u>Example</u>: Verify the result of Euler's theorem for $\overline{x}$ in R/pR where $R = \mathbb{F}_3[x]$ and $p = x^2 + x + 2$.

- It is straightforward to see that $p = x^2 + x + 2$ is irreducible in $\mathbb{F}_3[x]$, so R/pR is a field.
- We also know that the residue classes have the form $\overline{a + bx}$ for $a, b \in \mathbb{F}_3$. Thus, R/pR has 9 elements, 8 of which are units.
- To verify Euler's theorem we need to evaluate $\overline{x}^8$, which we can do using successive squaring: $\overline{x}^2 = \overline{2x+1}$, $\overline{x}^4 = (\overline{2x+1})^2 = \overline{2}$, and then $\overline{x}^8 = \overline{2}^2 = \overline{1}$.
- Thus, $\overline{x}^8 = \overline{1}$, meaning that $x^8 \equiv 1 \pmod{p}$, as dictated by Euler's theorem.

Euler and Fermat, VI

Although it is cheating a bit, we can obtain Fermat's little theorem quite easily using Euler's theorem.

Corollary (Fermat's Little Theorem)

If R is a Euclidean domain, $p \in R$ is a prime element, and the number of elements in R/pR is n, then $a^n \equiv a \pmod{p}$ for every $a \in R$.

Proof:

- Since R/pR is a field, the only nonunit is zero, so $\varphi(p) = n - 1$.
- Then by Euler's theorem, $a^{\varphi(p)} \equiv 1 \pmod{p}$ for every a that is a unit modulo p, so $a^n = a^{\varphi(p)+1} \equiv a \pmod{p}$ for such a.
- Since $a^n \equiv a \pmod{p}$ is also true when $p|a$, we see that it holds for every $a \in R$.

Euler and Fermat, VII: The Force Awakens

Example: Verify the result of Fermat's little theorem for $\overline{x}$ in R/pR where $R = \mathbb{F}_2[x]$ and $p = x^3 + x + 1$.

- It is straightforward to see that $p = x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, so R/pR is a field.
- We also know that the residue classes have the form $\overline{a + bx + cx^2}$ for $a, b, c \in \mathbb{F}_2$. Thus, R/pR has 8 elements.
- To verify Euler's theorem we need to evaluate $\overline{x}^8$, which we can do using successive squaring: $\overline{x}^2 = \overline{x^4}$, $\overline{x}^4 = (\overline{x^2})^2 = \overline{x^2 + x}$, and then $\overline{x}^8 = \overline{x^2 + x}^2 = \overline{x}$.
- Thus, $\overline{x}^8 = \overline{x}$, meaning that $x^8 \equiv x \pmod{p}$, as dictated by Fermat's little theorem.

Summary

We generalized the Chinese Remainder Theorem, Euler's Theorem, and Fermat's Little Theorem to the general setting R/pR where R is a Euclidean domain.

Next lecture: Factorization of polynomials in $F[x]$.