# Math 175 Lecture

Minh-Tam Trinh
*after* Ngô Bảo Châu

1 December 2015

## 1 Introduction

The final exam for this course, like the midterm exam, will focus on computations, not proofs. To this end, we have three sledgehammer theorems at our disposal:

1. The Chinese Remainder Theorem
2. The structure theorem for unit groups $U_m$.
3. Hensel's Theorem on lifting roots of polynomials modulo prime powers.

In this lecture, I will illustrate how these theorems relate to various exercises that appeared on Sets #5 and #6, as well as other standard questions.

## 2 The Chinese Remainder Theorem

### 2.1

**Theorem 2.1** (Chinese Remainder)**.** *If $m_1, \ldots, m_r \in \mathbb{N}$ are pairwise coprime, then the map*

$$\mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \tag{1}$$

*that sends $[a]_{m_1 \cdots m_r} \mapsto [a]_{m_1} \times \cdots \times [a]_{m_r}$ is a ring isomorphism.*

First, let us recall how to invert the map (1). That is, how can we construct, from pairwise coprime $m_1, \ldots, m_r \in \mathbb{N}$ and arbitrary $a_i \in \mathbb{Z}/m_i\mathbb{Z}$, an element $a \in \mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z}$ such that $a \equiv a_i \pmod{m_i}$ for all $i$? Yet another way of formulating this question is, we must solve the system

$$\begin{cases} x \equiv a_1 & \pmod{m_1} \\ \vdots & \\ x \equiv a_r & \pmod{m_r} \end{cases} \tag{2}$$

of linear congruences for $x$ modulo $m_1 \cdots m_r$.

It suffces to find $\delta_1, \ldots, \delta_r \in \mathbb{Z}$ such that

$$\delta_i \equiv \begin{cases} 1 & \pmod{m_i} \\ 0 & \pmod{m_j} \text{ for } j \neq i \end{cases} \tag{3}$$

because then we can take

$$a = a_1\delta_1 + \cdots + a_r\delta_r. \tag{4}$$

To get $\delta_i$, set $M_i = (m_1 \cdots m_r)/m_i$ and compute the multiplicative inverse of $M_i$ modulo $m_i$, which we can do because $\gcd(M_i, m_i) = 1$. If $N_i$ is a representative for the inverse, then $M_iN_i \equiv 1 \pmod{m_i}$, but at the same time, $M_iN_i \equiv 0 \pmod{m_j}$ for $j \neq i$ because $m_j \mid M_i$. So we can take $\delta_i = M_iN_i$.

## 2.2

Next, we review the two most important corollaries of the Chinese Remainder Theorem and their applications.

**Corollary 2.2** (Multiplicative Chinese Remainder)**.** *If $m_1, \ldots, m_r \in \mathbb{N}$ are pairwise coprime, then the map*

$$U_{m_1 \cdots m_r} \to U_{m_1} \times \cdots \times U_{m_r} \tag{5}$$

*that sends $[a]_{m_1 \cdots m_r} \mapsto [a]_{m_1} \times \cdots \times [a]_{m_r}$ is a group isomorphism.*

**Corollary 2.3.** *Suppose $m_1, \ldots, m_r \in \mathbb{N}$ are pairwise coprime. If $f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$, then:*

$$\{(x_1, \ldots, x_r) \text{ solving } f \text{ modulo } m_1 \cdots m_r\} = \bigcap_i \{(x_1, \ldots, x_r) \text{ solving } f \text{ modulo } m_i\}. \tag{6}$$

*That is, to solve $f$ modulo $m_1 \cdots m_r$ is to solve $f$ modulo each of $m_1, \ldots, m_r$ simultaneously.*

**Example 2.4.** If $a, m_1, \ldots, m_r \in \mathbb{N}$ are pairwise coprime, then $a$ is a quadratic residue modulo $m_1 \cdots m_r$ if and only if it is a quadratic residue modulo $m_i$ for each $i$. We can deduce this from either of Corollary 2.2 or 2.3.

**Example 2.5.** Exercise 5 on Set #6 was to solve the system

$$\left\{ \begin{array}{l} 2x + 3y \equiv 1 \\ 6x + 10y \equiv 2 \end{array} \right\} \pmod{24}. \tag{7}$$

In problems like this, we cannot just rescale both equations and subtract to eliminate one of the variables: Either way we do it, we have to rescale one of the equations by 3; but 3 is a zero-divisor modulo 12, so rescalng by 3 could potentially lose as much information as rescaling by 0. (However, it turns out that for this specific problem, no solutions are actually lost upon rescaling by 3, which gave the author great confusion during the grading process.)

Instead, the safe strategy is to break up 24 into $2^3 \cdot 3$ and solve the system modulo $2^3$ and 3 separately.

1. Modulo 8, the system is

   $$\left\{ \begin{array}{l} 2x + 3y \equiv 1 \\ 6x + 2y \equiv 2 \end{array} \right. \tag{8}$$

   Since 3 is invertible modulo 8, we can rescale the first congruence by 3 to get $6x + 9y \equiv 3$, which we then subtract from the second to get $7y \equiv 1 \pmod{8}$, whence $y \equiv 7 \pmod{8}$. Thus, $2x \equiv 1 - 3y \equiv -20 \equiv 4 \pmod{8}$, whence $x \equiv 2, 6 \pmod{8}$.

2. Modulo 3, the system is

   $$\left\{ \begin{array}{l} 2x \equiv 1 \\ 2y \equiv 1 \end{array} \right. \tag{9}$$

   The solution is $(x, y) \equiv (2, 2) \pmod{3}$.

Altogether, we must solve the systems

$$\left\{ \begin{array}{rl} x \equiv 2, 6 & \pmod{8} \\ x \equiv 2 & \pmod{3} \end{array} \right. \qquad \left\{ \begin{array}{rl} y \equiv 7 & \pmod{8} \\ y \equiv 2 & \pmod{3} \end{array} \right. \tag{10}$$

Ultimately, the only solution is $x \equiv 2, 14 \pmod{24}$ and $y \equiv 23 \pmod{24}$.

## 2.3

Exercise 3 on Set #6 was a generalization of the Chinese Remainder Theorem. Below, we restate the solution, then restate the restatement in a form closer to that of Theorem 2.1.

**Exercise 2.6.** The system of congruences

$$\begin{cases} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \end{cases} \tag{11}$$

has a solution in $x$ if and only if $a_1 \equiv a_2 \pmod{\gcd(m, m_2)}$, and in this case, $x$ is unique modulo $\mathrm{lcm}(m_1, m_2)$.

**Theorem 2.7** (Generalized Chinese Remainder)**.** *If $m_1, m_2 \in \mathbb{N}$, then the map*

(12)

$$\mathbb{Z}/\mathrm{lcm}(m_1, m_2)\mathbb{Z} \xrightarrow{\simeq} \{[a_1]_{m_1} \times [a_2]_{m_2} \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} : [a_1]_{\gcd(m_1,m_2)} = [b]_{\gcd(m_1,m_2)}\}$$

*that sends $[a]_{\mathrm{lcm}(m_1,m_2)} \mapsto [a]_{m_1} \times [a]_{m_2}$ is a bijection.*

If, in the statement of Theorem 2.7, we assume $m_1$ and $m_2$ are coprime, then $\mathrm{lcm}(m_1, m_2) = m_1 m_2$ and $\gcd(m_1, m_2) = 1$, so (12) simplifies to an isomorphism

$$\mathbb{Z}/m_1 m_2\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}. \tag{13}$$

Hence, the theorem does indeed generalize the $r = 2$ case of Theorem 2.1. It helps (me, at least) to visualize the general version in terms of the following diagram:

(14)

$$\begin{tikzcd}
& \mathbb{Z}/\mathrm{lcm}(m_1, m_2)\mathbb{Z} \arrow[dl] \arrow[dr] & \\
\mathbb{Z}/m_1\mathbb{Z} \arrow[dr] & & \mathbb{Z}/m_2\mathbb{Z} \arrow[dl] \\
& \mathbb{Z}/\gcd(m_1, m_2)\mathbb{Z} &
\end{tikzcd}$$

Translating the bijection in Theorem 2.7 to an "if and only if," the theorem states that, if we pick elements of the rings in the *left* and *right* corners, then they have a *unique* common lift to the *top* ring if and only if they have a common image in the *bottom* ring; otherwise, they do not have any lift to the top ring in common.

**Example 2.8.** Exercise 2 on Set #6 asked for all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 8 & \pmod{9} \\ x \equiv 31 & \pmod{33} \end{cases} \tag{15}$$

But $\gcd(9, 33) = 3$; we compute $8 \equiv 2 \pmod{3}$ and $31 \equiv 1 \pmod{3}$, so Theorem 2.7 says there are no solutions to this linear system.

**Example 2.9.** Exercise 1 on Set #6 asked for all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 10 & \pmod{24} \\ x \equiv 16 & \pmod{18} \end{cases} \tag{16}$$

We compute $\gcd(24, 18) = 6$; since $10 \equiv 4 \equiv 16 \pmod 6$, the system has a unique solution modulo $\operatorname{lcm}(24, 18) = 72$. We know any solution $x$ can be written in the form $10+24k = 16+18\ell$ for some $k, \ell \in \mathbb{Z}$. So we want to find all integers $k, \ell$ that solve $24k - 18\ell = 6$. We have

$$24k - 18\ell = 6 \iff 4k - 3\ell = 1. \tag{17}$$

When you plot this line in the $(k, \ell)$-plane, you see that it passes through $(1, 1)$, and more generally, the lattice points through which it passes are precisely the lattice points of the form $(1 + 3t, 1 - 4t)$ for some $t \in \mathbb{Z}$. Therefore, $x = 10 + 24(1 + 3t) = 16 + 18(1 - 4t)$ for some $t \in \mathbb{Z}$. We conclude that $x \equiv 34 \pmod{72}$.

**Example 2.10.** Suppose Exercise 1 on Set #6 had instead asked for all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 10 & \pmod{24} \\ x \equiv 16 & \pmod{18} \\ x \equiv 14 & \pmod{20} \end{cases} \tag{18}$$

To solve this triple congruence, we first solve the first two congruences simultaneously to get $x \equiv 34 \pmod{72}$. It then remains to solve the system

$$\begin{cases} x \equiv 34 & \pmod{72} \\ x \equiv 14 & \pmod{20} \end{cases} \tag{19}$$

We compute $\gcd(72, 20) = 4$; since $34 \equiv 2 \equiv 14 \pmod 4$, the system has a unique solution modulo $\operatorname{lcm}(72, 20) = 360$. It must take the form $34 + 72k = 14 + 20\ell$, which simplifies to $18k - 5\ell = -5$. The integer solutions to this system are $(k, \ell) = (5t, 1 - 18t)$. So the solution to the original system is $x \equiv 34 \pmod{360}$.

## 3 The Structure of Unit Groups

**Theorem 3.1** (Structure of Unit Groups). *If $p$ is a prime and $e \in \mathbb{N}$, then:*

$$U_{p^e} \simeq \begin{cases} 0 & p = 2,\ e = 1 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z} & p = 2,\ e \geq 2 \\ \mathbb{Z}/\varphi(p^e)\mathbb{Z} & p \text{ is odd} \end{cases} \tag{20}$$

*Moreover:*

1. *$U_{2^e}$ is always generated by $[-1]_{2^e}$ and $[5]_{2^e}$.*
2. *For odd $p$, if $[a]_{p^2}$ generates $U_{p^2}$, then $[a]_{p^e}$ generates $U_{p^e}$.*

*In particular, $U_2, U_4$, and $U_{p^e}$ for odd $p$ are cyclic.*

Theorem 3.1 tells us the structure of $U_m$ for prime-power $m$. Corollary 2.2 tells us that for general $m$, if $m = p_1^{e_1} \cdots p_r^{e_r}$ is the unique prime factorization of $m$, then

$$U_m \simeq U_{p_1^{e_1}} \times \cdots \times U_{p_r^{e_r}}. \tag{21}$$

So together, these two results describe the structure of $U_m$ for arbitrary $m$.

**Example 3.2.** If you want to find the orders of all the elements of $U_9$, as in Exercise 6.1 of [JJ], you <u>don't</u> need to write out all the powers of each element separately.

First, find a primitive root for $U_9$, such as $[2]_9$. (Admittedly, there is no surefire algorithm for finding a primitive root in general, but checking that a given element is a primitive root is not too hard.) In writing out the first $\varphi(9) = 6$ powers of $[2]_9$, we write out an isomorphism $\mathbb{Z}/6\mathbb{Z} \to U_9$:

(22)

| $\mathbb{Z}/6\mathbb{Z}$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $U_9$ | 1 | 2 | 4 | 8 | 7 | 5 |

But, for example, it's apparent that the order of 2 in $\mathbb{Z}/6\mathbb{Z}$ is 3, so correspondingly, the order of 4 in $U_9$ is 3. And so on.

**Example 3.3.** Exercise 2(1) on Set #5 asked you to solve congruences of the form

$$x^n \equiv a \pmod{17} \tag{23}$$

using the fact that $U_{17} \simeq \mathbb{Z}/16\mathbb{Z}$. Many people solved this problem incorrectly, so it is important that we carefully review the correct solution.

An isomorphism $\psi : \mathbb{Z}/16\mathbb{Z} \to U_{17}$ is given by following table:

(24)

| $\mathbb{Z}/16\mathbb{Z}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $U_{17}$ | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 |

To solve a congruence of the form (23) using this table:

1. Applying $\psi^{-1}$ to both sides, we obtain $n\psi^{-1}(z) \equiv \psi^{-1}(a) \pmod{16}$.
2. Solve this linear congruence modulo 16 for $\psi^{-1}(z)$.
3. Apply $\psi$ to recover $z$.

For example, suppose you want to solve

$$z^{12} \equiv 16 \pmod{17}. \tag{25}$$

We have $12\psi^{-1}(z) \equiv 8 \pmod{16}$. Dividing through by 4, we have $3\psi^{-1}(z) \equiv 2 \pmod{4}$, giving $\psi^{-1}(z) \equiv 2 \pmod{4}$. Therefore, $\psi^{-1}(z) \equiv 2, 6, 10, 14 \pmod{16}$, whence $z \equiv 9, 15, 8, 2 \pmod{17}$. Several people only found one solution, not all four.

**Example 3.4.** Suppose $p$ is an odd prime and $e \in \mathbb{N}$. We will prove that $-1$ is a quadratic residue modulo $p^e$ if and only if $p \equiv 1 \pmod{4}$, using the structure theorem.

Under the isomorphism $U_{p^e} \simeq \mathbb{Z}/\varphi(p^e)\mathbb{Z}$, we have a correspondence

$$[-1]_{p^e} \leftrightarrow [\varphi(p^e)/2]_{\varphi(p^e)}, \tag{26}$$

because these are the <u>unique</u> elements of order 2 in their respective groups. So we have a correspondence

$$\text{solving } x^2 \equiv -1 \pmod{p^e} \text{ for } x \iff \text{solving } 2y \equiv \frac{\varphi(p^e)}{2} \pmod{\varphi(p^e)} \text{ for } y. \tag{27}$$

Note that the right-hand side makes sense because $\varphi(p^e) = p^{e-1}(p-1)$ is always even. For the right-hand side to be solvable, it's <u>necessary</u> that $\varphi(p^e)/2$ be even, and it's <u>sufficient</u> that $\varphi(p^e)/2$ be even because then we can take $y \equiv \varphi(p^e)/4$. In turn, $\varphi(p^e)/2$ is even if and only if $(p-1)/2$ is even, i.e., $p \equiv 1 \pmod{4}$.

## 4 Hensel Lifting

**Theorem 4.1** (Hensel)**.** *Let $f(x) \in \mathbb{Z}[x]$. Suppose that for some $e \in \mathbb{N}$ and $[a]_{p^e} \in \mathbb{Z}/p^e\mathbb{Z}$, we know $a$ is a root of $f$ modulo $p^e$.*

1. *If $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique lift of $[a]_{p^e}$ to $\mathbb{Z}/p^{e+1}\mathbb{Z}$ that is a root of $f$.*
2. *If $f'(a) \equiv 0 \pmod{p}$, then either every lift, or no lift, of $[a]_{p^e}$ to $\mathbb{Z}/p^{e+1}\mathbb{Z}$ is a root of $f$.*

If we are in the "good" case where $f'(a) \not\equiv 0$, then we can explicitly compute the unique lift that is still a root of $f$, by the following technique: First, we can write the lift in the form $a + p^e t$. Next, we have congruences

$$0 \equiv f(a + p^e t) \equiv f(a) + f'(a)p^e t \pmod{p^{e+1}}. \tag{28}$$

Indeed, the left-hand side is just the fact that $x + p^e t$ is still a root; the right-hand side uses the Taylor-expansion trick that Professor Ngô showed us before.

**Example 4.2.** Let

$$f(x) = x^2 + 1. \tag{29}$$

We know $[4]_{17}$ is a root of $f$ modulo 17 and $f'(4) \equiv 2(4) \equiv 8 \not\equiv 0 \pmod{17}$, so Hensel's Theorem says there is a unique lift of $[4]_{17}$ to a root of $f$ modulo $17^2$. It must take the form $4 + 17t$, where $t$ must satisfy

$$0 \equiv 17 + 8 \cdot 17 \cdot t \pmod{17^2}. \tag{30}$$

That is, $17^2$ divides $17(1 + 8t)$, which occurs if and only if 17 divides $1 + 8t$. We deduce that $t \equiv 2 \pmod{17}$, whence the lift is $4 + 17t \equiv 4 + 34 \equiv 38 \pmod{17^2}$.

**Example 4.3.** We will reprove the result of Example 3.4 using Hensel's Theorem and the $e = 1$ case of the structure theorem, instead of the full structure theorem. Recall that the result was: If $p$ is an odd prime and $e \in \mathbb{N}$, then $x^2 \equiv -1 \pmod{p^e}$ is solvable for $x$ if and only if $p \equiv 1 \pmod{4}$.

Assume we know the result holds for $e = 1$, e.g., by Corollary 7.7 of [JJ]. For all $e \geq 2$, the <u>un</u>solvability of $x^2 \equiv -1$ modulo $p$ implies its <u>un</u>solvability modulo $p^e$, so it remains to show that the solvability of $x^2 \equiv -1$ modulo $p$ implies its solvability modulo $p^e$.

Let $f(x) = x^2 + 1$ once again. Suppose there exists $x_1 \in \mathbb{Z}$ such that $f(x_1) \equiv 0 \pmod{p}$. We will show by induction on $e$ that, for all $e \geq 1$, there exists $x_e \in \mathbb{Z}$ such that

1. $f(x_e) \equiv 0 \pmod{p^e}$.
2. $x_e \not\equiv 0 \pmod{p}$.

The base case holds because we've assumed the existence of $x_1$ as a hypothesis, and since $f(0) \not\equiv 0 \pmod{p}$, we know that $x_1 \not\equiv 0 \pmod{p}$.

Suppose $x_e$ satisfies conditions (1) and (2). By condition (2) and $p$ being odd, $f'(x_e) = 2x_e \not\equiv 0 \pmod{p}$, so by Hensel's Theorem, there exists $x_{e+1} \in \mathbb{Z}$ such that $f(x_{e+1}) \equiv 0 \pmod{p^{e+1}}$ and $x_{e+1} \equiv x_e \pmod{p^e}$. In particular, $x_{e+1} \equiv x_e \not\equiv 0 \pmod{p}$, which completes the induction.

## Reference

[JJ] G. A. Jones & J. M. Jones. *Elementary Number Theory.* Springer-Verlag (1998).