Math 115. Slides from the Lecture of September 24

This handout contains the slides from the lecture of September 24.

Let's look at the equation $x^2 \equiv 1 \pmod{15}$.

This has four solutions: $x \equiv \pm 1, \pm 4 \pmod{15}$.

Recall Theorem 2.3(3): Let $m_1, \dots, m_r \in \mathbb{Z}_{>0}$, with $r \in \mathbb{Z}_{>0}$. Then $x \equiv y \pmod{m_i}$ for all $i = 1, \dots, r$ if and only if $x \equiv y \pmod{\operatorname{lcm}(m_1, \dots, m_r)}$.

By this theorem, $x^2 \equiv 1 \pmod{15}$ is equivalent to $x^2 \equiv 1 \pmod 3$ and $x^2 \equiv 1 \pmod 5$.

More generally:

x mod 15	x mod 3	x mod 5
1	1	1
4	1	4 $(\equiv -1)$
11 $(\equiv -4)$	2 $(\equiv -1)$	1
14 $(\equiv -1)$	2 $(\equiv -1)$	4 $(\equiv -1)$

So, we can "mix and match" solutions modulo 3 and solutions modulo 5 to get solutions modulo 15.

A More General Question

Given $m_1, \dots, m_r \in \mathbb{Z}_{>0}$ and $a_1, \dots, a_r \in \mathbb{Z}$, what can we say about integer solutions x to the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \tag{*}$$

The Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem). *Let $a_1, \dots, a_r \in \mathbb{Z}$ be given, and assume that $m_1, \dots, m_r$ are pairwise relatively prime positive integers. Let $m = m_1 \cdots m_r$. Then the system (*) has solutions. Moreover, if $x_0 \in \mathbb{Z}$ is one such solution, then $x \in \mathbb{Z}$ is a solution if and only if $x \equiv x_0 \pmod m$.*

Proof. **Case I:** $r = 1$**.** This is trivial.

Case II: $r = 2$**.** Since $\gcd(m_1, m_2) = 1$, there are integers c_1 and c_2 such that $c_1 m_1 + c_2 m_2 = 1$. Then

$$\begin{aligned} c_1 m_1 &\equiv 0 \pmod{m_1} \\ c_1 m_1 &\equiv 1 \pmod{m_2} \end{aligned} \qquad \text{and} \qquad \begin{aligned} c_2 m_2 &\equiv 1 \pmod{m_1} \\ c_2 m_2 &\equiv 0 \pmod{m_2} \end{aligned}$$

Let $x_0 = a_1c_2m_2 + a_2c_1m_1$. Then

$$\begin{aligned} x_0 &\equiv a_1 \cdot 1 + a_2 \cdot 0 = a_1 \pmod{m_1} \qquad \text{and} \\ x_0 &\equiv a_1 \cdot 0 + a_2 \cdot 1 = a_2 \pmod{m_2} , \end{aligned}$$

so it is a solution of (*).

Now let $x \in \mathbb{Z}$. Then:

$$\begin{aligned} x \text{ is another solution} &\iff x \equiv a_i \pmod{m_i} \text{ for all } i \\ &\iff x \equiv x_0 \pmod{m_i} \text{ for all } i \\ &\iff x \equiv x_0 \pmod{m} . \end{aligned}$$

This gives the last sentence.

The above is true for all r , but we still need to prove the main part for arbitrary r . This can be done by induction on r .

Case III: $r > 2$. This will be done by induction. The base case $r = 2$ has been done already.

So, assume that $r > 2$ and that the theorem is true when r is replaced by $r - 1$.

By the inductive hypothesis there is an a_0 such that $a_0 \equiv a_i \pmod{m_i}$ for all $i < r$. By the $r = 2$ case there is an integer x_0 such that $x_0 \equiv a_0 \pmod{m_1 \cdots m_{r-1}}$ and $x_0 \equiv a_r \pmod{m_r}$. This integer satisfies all parts of the system (*), because for all $i < r$ we have

$$x_0 \equiv a_0 \equiv a_i \pmod{m_i} ,$$

and we still have $x_0 \equiv a_r \pmod{m_r}$. □

How To Compute???

Method 1: Follow the above proof (or the book's proof).

Example. Solve the congruences

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod 9 . \end{aligned}$$

Noting that

$$4 \cdot 9 - 5 \cdot 7 = 1 ,$$

we have

$$\begin{aligned} 36 &\equiv 1 \pmod 7 \\ 36 &\equiv 0 \pmod 9 \end{aligned} \qquad \text{and} \qquad \begin{aligned} -35 &\equiv 0 \pmod 7 \\ -35 &\equiv 1 \pmod 9 \end{aligned}$$

Then we can let

$$x_0 = 2(36) + 3(-35) = 72 - 105 = -33$$

to conclude that the solution set is all integers x such that $x \equiv -33 \pmod{63}$ (or $x \equiv 30 \pmod{63}$).

Method 2: A separate method from the book. (This method does not require that $m_1, \dots, m_r$ be pairwise relatively prime.)

The first congruence $x \equiv 2 \pmod 7$ is equivalent to $x = 7u + 2$ with $u \in \mathbb{Z}$.

Substitute this value for x into the second congruence $x \equiv 3 \pmod 9$:

$$\begin{aligned} 2 + 7u &\equiv 3 \pmod 9 \\ 7u &\equiv 1 \pmod 9 \end{aligned}$$

Using the equation $4 \cdot 9 - 5 \cdot 7 = 1$, we find that $7^{-1} \equiv -5 \equiv 4 \pmod 9$. So, multiply both sides by 4:

$$\begin{aligned} 28u &\equiv 4 \pmod 9 \\ u &\equiv 4 \pmod 9 \\ u &= 9v + 4 \qquad \text{with } v \in \mathbb{Z}\,. \end{aligned}$$

Now substitute this value ($u = 9v + 4$) into $x = 7u + 2$ to get the answer:

$$x = 7(9v + 4) + 2 = 63v + 28 + 2 = 63v + 30\,.$$

We conclude that x satisfies the two given congruences if and only if $x \equiv 30 \pmod{63}$.

Techniques of Numerical Calculation

The main points of Section 2.4 (and related facts) for us are:

A. "Polynomial time"

Definition. An algorithm **runs in polynomial time** if the time it takes is at most some polynomial function of *the length of the input*.

Examples:

- Addition: Adding an n-digit number and an m-digit number takes at most $\max\{n, m\} + 1$ steps. This is polynomial time (actually, linear time).
- Multiplication: $2mn$, so polynomial time (quadratic)
- Division (division algorithm): likewise
- Euclidean algorithm: The number of iterations is linear in the number of digits of the smaller of the two numbers. Each iteration takes time quadratic in the length of the input, so this takes place in polynomial time.
- Factoring a number n by trial division takes $\sqrt{n}$ divisions. But:

$$\sqrt{n} \approx 3^{\text{number of digits in } n}\,.$$

So: exponential time.

B. Computing $a^k \underline{\mathrm{mod}}\, m$ in polynomial time.

See the algorithm in the book.

C. Primality testing: Given an integer $m > 0$, is it prime?

Mostly this relies on Fermat's Little Theorem:
If there is an integer a such that $0 < a < m$ and $a^{m-1} \not\equiv 1 \pmod{m}$, then m is not prime.
For each such a, this can be tested in polynomial time, by (B).

Definition. Let $a \in \mathbb{Z}$ with $a > 1$. Then an integer $m > 1$ is a *(weak) probable prime to the base* a if $a^{m-1} \equiv 1 \pmod{m}$, and is a *(weak) pseudoprime to the base* a if in addition m is not prime.

Definition. A **Carmichael number** is a composite number m which is a weak pseudoprime to the base a for all integers a relatively prime to m.

The smallest Carmichael number is 561.

A better primality test.

Definition. Let m be an integer > 1 and write $m - 1 = 2^j d$ with $j \in \mathbb{N}$ and d odd. Let $a \in \mathbb{Z}$ with $a > 1$. Then m is a *strong probable prime to the base* a if $a^{m-1} \equiv 1 \pmod{m}$, and the last element in the sequence

$$a^d, a^{2d}, a^{4d}, \dots, a^{2^j d} = a^{m-1}$$

which is $\not\equiv 1 \pmod{m}$ (if any) is $\equiv -1 \pmod{m}$. (So if $a^d \equiv 1 \pmod{m}$ then it is a strong probable prime.)
Strong pseudoprime to the base a is defined similarly.

D. Other tidbits:

- There is a test for primality that runs in polynomial time (AKS, 2002).
- Factoring a number is *not* known to have a polynomial-time algorithm.