Notes for Lecture 10

9 Chinese remainder theorem

Example 88. (warmup)

(a) If $x \equiv 3 \pmod{10}$, what can we say about $x \pmod{5}$?

(b) If $x \equiv 3 \pmod{7}$, what can we say about $x \pmod{5}$?

Solution.

(a) If $x \equiv 3 \pmod{10}$, then $x \equiv 3 \pmod{5}$.
[Why?! Because $x \equiv 3 \pmod{10}$ if and only if $x = 3 + 10m$, which modulo 5 reduces to $x \equiv 3 \pmod{5}$.]

(b) Absolutely nothing! $x = 3 + 7m$ can be anything modulo 5 (because $7 \equiv 2$ is invertible modulo 5).

Example 89. If $x \equiv 3 \pmod{5}$, what can we say about $x \pmod{15}$?

Solution. $x \equiv 3, 8, 13 \pmod{15}$

Example 90. If $x \equiv 32 \pmod{35}$, then $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Why?! As in the first part of the warmup, if $x \equiv 32 \pmod{35}$, then $x \equiv 32 \pmod{5}$ and $x \equiv 32 \pmod{7}$.

The Chinese remainder theorem says that this can be reversed!

That is, if $x \equiv 2 \pmod{5}$ and $x \equiv 4 \pmod{7}$, then the value of x modulo $5 \cdot 7 = 35$ is determined.
[How to find the value $x \equiv 32 \pmod{35}$ is discussed in the next example.]

Example 91. Solve $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Solution. $x \equiv 2 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 5}}_{3} + 4 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 7}}_{3} \equiv 42 + 60 \equiv 32 \pmod{35}$

Important comment. Can you see how we need 5 and 7 to be coprime here?

Brute force solution. Note that, while in principle we can always perform a brute force search, this is not practical for larger problems. Here, if x is a solution, then so is $x + 35$. So we only look for solutions modulo 35.
Since $x \equiv 4 \pmod{7}$, the only candidates for solutions are $4, 11, 18, \ldots$ Among these, we find $x = 32$.
[We can also focus on $x \equiv 2 \pmod{5}$ and consider the candidates $2, 7, 12, \ldots$, but that is even more work.]

Example 92. Solve $x \equiv 2 \pmod{3}$, $x \equiv 1 \pmod{5}$.

Solution. $x \equiv 2 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 3}}_{-1} + 1 \cdot 3 \cdot \underbrace{3^{-1}_{\bmod 5}}_{2} \equiv -10 + 6 \equiv 11 \pmod{15}$

Theorem 93. (Chinese Remainder Theorem) Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad \ldots, \quad x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$.

In other words. The Chinese remainder theorem provides a bijective (i.e., 1-1 and onto) correspondence

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod{n} \\ x \pmod{m} \end{bmatrix}.$$

For instance. Let's make the correspondence explicit for $n = 2$, $m = 3$:

$0 \mapsto \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $1 \mapsto \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $2 \mapsto \begin{bmatrix} 0 \\ 2 \end{bmatrix}$, $3 \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $4 \mapsto \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $5 \mapsto \begin{bmatrix} 1 \\ 2 \end{bmatrix}$

Armin Straub
straub@southalabama.edu

Example 94. Solve $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.

Solution. $x \equiv 1 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)^{-1}_{\bmod 4}]}_{3} + 2 \cdot 4 \cdot 7 \cdot \underbrace{[(4 \cdot 7)^{-1}_{\bmod 5}]}_{2} + 3 \cdot 4 \cdot 5 \cdot \underbrace{[(4 \cdot 5)^{-1}_{\bmod 7}]}_{-1}$
$\equiv 105 + 112 - 60 = 157 \equiv 17 \pmod{140}$.

Alternative solution. Alternatively, we can solve the problem in two steps:

First, we solve $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$ and get $x \equiv 1 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 4}}_{1} + 2 \cdot 4 \cdot \underbrace{4^{-1}_{\bmod 5}}_{-1} \equiv 5 - 8 = -3 \pmod{20}$.

Then, we solve $x \equiv -3 \pmod{20}$, $x \equiv 3 \pmod{7}$ to get $x \equiv -3 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 20}}_{3} + 3 \cdot 20 \cdot \underbrace{20^{-1}_{\bmod 7}}_{-1} \equiv 17 \pmod{140}$.

Silicon slave labor. Once you are comfortable doing it by hand, you can easily let Sage do the work for you:

```
Sage] crt([1,2,3], [4,5,7])
```

17

Example 95.

(a) Let $p > 3$ be a prime. Show that $x^2 \equiv 9 \pmod{p}$ has exactly two solutions (i.e. ± 3).

(b) Let p, $q > 3$ be distinct primes. Show that $x^2 \equiv 9 \pmod{pq}$ always has exactly four solutions (± 3 and two more solutions $\pm a$).

Solution.

(a) If $x^2 \equiv 9 \pmod{p}$, then $0 \equiv x^2 - 9 = (x-3)(x+3) \pmod{p}$. Since p is a prime it follows that $x - 3 \equiv 0 \pmod{p}$ or $x + 3 \equiv 0 \pmod{p}$. That is, $x \equiv \pm 3 \pmod{p}$.

(b) By the CRT, we have $x^2 \equiv 9 \pmod{pq}$ if and only if $x^2 \equiv 9 \pmod{p}$ and $x^2 \equiv 9 \pmod{q}$. Hence, $x \equiv \pm 3 \pmod{p}$ and $x \equiv \pm 3 \pmod{q}$. These combine in four different ways.

For instance, $x \equiv 3 \pmod{p}$ and $x \equiv 3 \pmod{q}$ combine to $x \equiv 3 \pmod{pq}$. However, $x \equiv 3 \pmod{p}$ and $x \equiv -3 \pmod{q}$ combine to something modulo pq which is different from 3 or -3.

Why primes >3? Why did we exclude the primes 2 and 3 in this discussion?

Comment. There is nothing special about 9. The same is true for $x^2 \equiv a^2 \pmod{pq}$ for each integer a.

Example 96. Determine all solutions to $x^2 \equiv 9 \pmod{35}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 9 \pmod{35} \\ \iff & x^2 \equiv 9 \pmod{5} \text{ and } x^2 \equiv 9 \pmod{7} \\ \iff & x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{7} \end{aligned}$$

The two obvious solutions modulo 35 are ± 3. To get one of the two additional solutions, we solve $x \equiv 3 \pmod{5}$, $x \equiv -3 \pmod{7}$. [Then the other additional solution is the negative of that.]

$x \equiv 3 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 5}}_{3} - 3 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 7}}_{3} \equiv 63 - 45 \equiv -17 \pmod{35}$

Hence, the solutions are $x \equiv \pm 3 \pmod{35}$ and $x \equiv \pm 17 \pmod{35}$.

Example 97. (review) Solve $x \equiv 2 \pmod{7}$, $x \equiv 3 \pmod{11}$.

Solution. $x \equiv 2 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} + 3 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} \equiv 44 - 63 \equiv 58 \pmod{77}$

Example 98. (review) Determine all solutions to $x^2 \equiv 4 \pmod{77}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 4 \pmod{77} \\ \iff\ & x^2 \equiv 4 \pmod{7} \text{ and } x^2 \equiv 4 \pmod{11} \\ \iff\ & x \equiv \pm 2 \pmod{7} \text{ and } x \equiv \pm 2 \pmod{11} \end{aligned}$$

Hence, there are four solutions modulo 77: $\pm 2, \pm a$. To find a, we solve $x \equiv 2 \pmod{7}$, $x \equiv -2 \pmod{11}$.

$x \equiv 2 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} - 2 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} \equiv 44 + 42 \equiv 9 \pmod{77}$

Hence, the four solutions are $x \equiv \pm 2, \pm 9 \pmod{77}$.

Example 99. By the Chinese remainder theorem there is a bijective correspondence

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod{n} \\ x \pmod{m} \end{bmatrix}.$$

Here's a graphical representation for $n = 3$, $m = 5$. Do you see the pattern?

		(mod 5)				
		0	1	2	3	4
(mod 3)	0	0	6		3	
	1		1	$\ddots$		4
	2	5		2	$\ddots$	

$\rightsquigarrow$

		(mod 5)				
		0	1	2	3	4
(mod 3)	0	0	6	12	3	9
	1	10	1	7	13	4
	2	5	11	2	8	14

Example 100. Solve $x \equiv 2 \pmod{3}$, $3x \equiv 2 \pmod{5}$, $5x \equiv 2 \pmod{7}$.

Solution. Note that $3^{-1} \equiv 2 \pmod{5}$ and $5^{-1} \equiv 3 \pmod{7}$.

Hence, we can simplify the congruences to $x \equiv 2 \pmod{3}$, $x \equiv 2 \cdot 2 \equiv -1 \pmod{5}$, $x \equiv 2 \cdot 3 \equiv -1 \pmod{7}$.

Using the CRT, $x \equiv 2 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)^{-1}_{\bmod 3}]}_{2} - 1 \cdot 3 \cdot 7 \cdot \underbrace{[(3 \cdot 7)^{-1}_{\bmod 5}]}_{1} - 1 \cdot 3 \cdot 5 \cdot \underbrace{[(3 \cdot 5)^{-1}_{\bmod 7}]}_{1}$

$\equiv 140 - 21 - 15 = 104 \equiv -1 \pmod{105}$.

Note. Can you see how we could have totally gotten that answer without the CRT computation?

Example 101. How many solutions does $x^2 \equiv 9 \pmod{M}$ have for $M = 55$? For $M = 385$? For $M = 110$? For $M = 105$?

Solution.

(a) $M = 55 = 5 \cdot 11$. There are 2 solutions modulo 5 and 2 solutions modulo 11. By the CRT, these combine to $2 \cdot 2 = 4$ solutions modulo 55.

(b) $M = 385 = 5 \cdot 7 \cdot 11$. There are 2 solutions modulo 5, 2 solutions modulo 7, and 2 solutions modulo 11. By the CRT, these combine to $2 \cdot 2 \cdot 2 = 8$ solutions modulo 385.

(c) $M = 110 = 2 \cdot 5 \cdot 11$. There is 1 solution modulo 2 (why?!), 2 solutions modulo 5, and 2 solutions modulo 11. By the CRT, these combine to $1 \cdot 2 \cdot 2 = 4$ solutions modulo 110.

(d) $M = 105 = 3 \cdot 5 \cdot 7$. There is 1 solution modulo 3 (why?!), 2 solutions modulo 5, and 2 solutions modulo 7. By the CRT, these combine to $1 \cdot 2 \cdot 2 = 4$ solutions modulo 105.

Armin Straub
straub@southalabama.edu

10 Euler's phi function

Definition 102. **Euler's phi function** $\phi(n)$ denotes the number of integers in $\{1,2,\ldots,n\}$ that are coprime to n.

[For $n>1$, we might as well replace $\{1,2,\ldots,n\}$ with $\{1,2,\ldots,n-1\}$.]

Important comment. In other words, $\phi(n)$ counts how many numbers are invertible modulo n.

Example 103. Compute $\phi(n)$ for $n=1,2,\ldots,8$.

Solution. $\phi(1)=1$, $\phi(2)=1$, $\phi(3)=2$, $\phi(4)=2$, $\phi(5)=4$, $\phi(6)=2$, $\phi(7)=6$, $\phi(8)=4$.

Observation 1. $\phi(n)=n-1$ if and only if n is a prime.

This is true because $\phi(n)=n-1$ if and only if n is coprime to all of $\{1,2,\ldots,n-1\}$.

Observation 2. If p is a prime, then $\phi(p^k)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right)$.

This is true because, if p is a prime, then $n=p^k$ is coprime to all $\{1,2,\ldots,p^k\}$ except $p,2p,\ldots,p^k$.

Theorem 104.

(a) $\phi(n)=n-1$ if and only if n is a prime.

(b) If p is a prime, then $\phi(p^k)=p^k-\frac{p^k}{p}=p^k\left(1-\frac{1}{p}\right)$.

(c) ϕ is multiplicative, that is, $\phi(nm)=\phi(n)\phi(m)$ whenever n,m are coprime.

(d) $\boxed{\text{If the prime factorization of } n \text{ is } n=p_1^{k_1}\cdots p_r^{k_r}, \text{ then } \phi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).}$

Proof.

(a) $\phi(n)=n-1$ if and only if n is coprime to all of $\{1,2,\ldots,n-1\}$. That's true for n precisely when it is a prime.

(b) If p is a prime, then $n=p^k$ is coprime to all $\{1,2,\ldots,p^k\}$ except $p,2p,\ldots,p^k$.

(c) Note that a is invertible modulo nm if and only if a is invertible modulo both n and m.

The claim therefore follows from the Chinese remainder theorem which provides a bijective (i.e., 1-1 and onto) correspondence

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod{n} \\ x \pmod{m} \end{bmatrix}.$$

Alternatively, our book contains a direct proof (page 133).

(d) Using the two previous parts, we have

$\phi(n)=\phi(p_1^{k_1})\cdots\phi(p_r^{k_r})=p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).$ □

Example 105. Compute $\phi(1000)$.

Solution. $\phi(1000)=\phi(2^3\cdot 5^3)=1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=400$.

Alternatively. $\phi(1000)=\phi(2^3)\cdot\phi(5^3)=(8-4)(125-25)=400$

Armin Straub
straub@southalabama.edu

Example 106. (extra)

(a) Solve $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{25}$.

(b) Solve $x \equiv -1 \pmod{4}$, $x \equiv 2 \pmod{7}$, $x \equiv 0 \pmod{9}$.

Solution. (final answer only)

(a) $x \equiv 78 \pmod{100}$

(b) $x \equiv 135 \pmod{252}$

Example 107. Compute $\phi(980)$.

Solution. $\phi(980) = \phi(2^2 \cdot 5 \cdot 7^2) = (2^2 - 2)(5 - 1)(7^2 - 7) = 336$.

Example 108. Determine all solutions to $x^2 \equiv 9 \pmod{110}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 9 \pmod{110} \\ \iff & x^2 \equiv 9 \pmod{2} \text{ and } x^2 \equiv 9 \pmod{5} \text{ and } x^2 \equiv 9 \pmod{11} \\ \iff & x \equiv \pm 3 \pmod{2} \text{ and } x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{11} \\ \iff & x \equiv 1 \pmod{2} \text{ and } x \equiv \pm 3 \pmod{5} \text{ and } x \equiv \pm 3 \pmod{11} \end{aligned}$$

Let us write down all possible four combinations:

solution #1	solution #2	solution #3	solution #4
$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{2}$	$x \equiv 1 \pmod{2}$
$x \equiv 3 \pmod{5}$	$x \equiv 3 \pmod{5}$	$x \equiv -3 \pmod{5}$	$x \equiv -3 \pmod{5}$
$x \equiv 3 \pmod{11}$	$x \equiv -3 \pmod{11}$	$x \equiv 3 \pmod{11}$	$x \equiv -3 \pmod{11}$
$x \equiv 3 \pmod{110}$	$x \equiv a \pmod{110}$	$x \equiv -a \pmod{110}$	$x \equiv -3 \pmod{110}$

To get the non-obvious solution a, we solve $x \equiv 1 \pmod{2}$, $x \equiv 3 \pmod{5}$, $x \equiv -3 \pmod{11}$.

$$x \equiv 1 \cdot 55 \cdot \underbrace{55^{-1}_{\bmod 2}}_{1} + 3 \cdot 22 \cdot \underbrace{22^{-1}_{\bmod 5}}_{-2} - 3 \cdot 10 \cdot \underbrace{10^{-1}_{\bmod 11}}_{-1} \equiv 55 - 132 + 30 \equiv -47 \pmod{110}$$

Hence, the solutions are $x \equiv \pm 3 \pmod{110}$ and $x \equiv \pm 47 \pmod{110}$.

11 Using Sage as a fancy calculator

Any serious number theory applications, such as those in cryptography, involve computations that need to be done by a machine. Let us see how to use the open-source computer algebra system **Sage** to do basic computations for us.

Sage is freely available at sagemath.org. Instead of installing it locally (it's huge!) we can conveniently use it in the cloud at cocalc.com from any browser.

Sage is built as a **Python** library, so any Python code is valid. For starters, we will use it as a fancy calculator.

Example 109. Let's start with some basics.

```
Sage] 17 % 12
```

5

```
Sage] (1 + 5) % 2  # don't forget the brackets
```

0

```
Sage] inverse_mod(17, 23)
```

19

```
Sage] xgcd(17, 23)
```

$(1, -4, 3)$

```
Sage] -4*17 + 3*23
```

1

Example 110. Can you figure out what is being computed here?

```
Sage] crt([2,-2], [7,11])
```

9

Example 111. Why is the following bad?

```
Sage] 3^1003 % 101
```

27

The reason is that this computes 3^{1003} first, and then reduces that huge number modulo 101:

```
Sage] 3^1003
```

3569591212598177919604229201330789788106639488430800052695284994212437212836103228760\
01447396641767302556399781555972361067577371671671062036425358196474919874574608035466\
17047063989041820507144085408031748926871104815910218235498276622866724603402112436668\
09387969298949770468720050187071564942882735677962417251222021721836167242754312973216\
80102291029227131545307753863985171834477895265551139587894463150442112884933077598746\
041251617347746428658788556867377476037709094002 7

We know how to avoid computing huge intermediate numbers. Sage does the same if we instead use something like:

```
Sage] power_mod(3, 1003, 101)
```

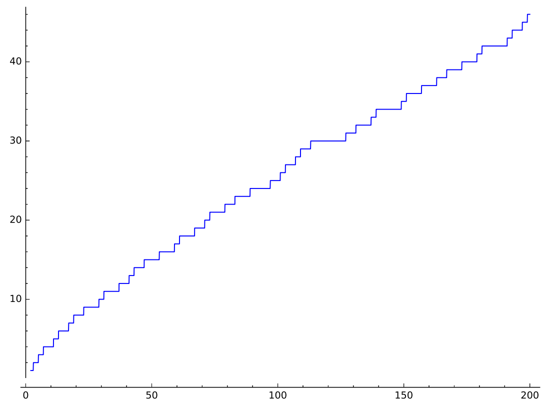
27

Example 112. Playing with the prime number theorem in Sage:

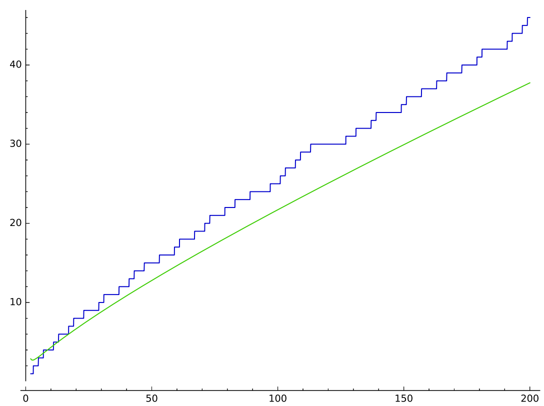
```
Sage] prime_pi(10)
```

4

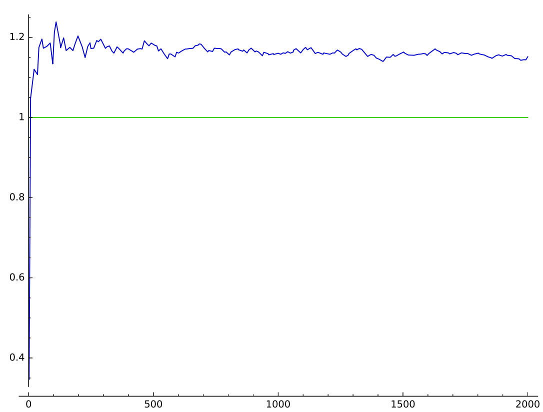
```
Sage] plot(prime_pi(x), 2, 200)
```




```
Sage] plot([prime_pi(x),x/ln(x)], 2, 200)
```




```
Sage] plot([prime_pi(x)/(x/ln(x)), 1], 2, 2000)
```



Comment. As the final plot suggests, the quotient of $\pi(x)$ and $x/\ln(x)$ indeed approaches 1 from above. This is slightly stronger than the PNT, which only claims that the quotient approaches 1.

In particular, as the previous plot suggests, for large x, $x/\ln(x)$ is always an underestimate for $\pi(x)$ (though looking at a plot like this can be very misleading).

Armin Straub
straub@southalabama.edu