Review. Prime number theorem

Theorem 33. The gaps between primes can be arbitrarily large.

Proof. Indeed, for any integer $n>1$,

$$n!+2, \quad n!+3, \quad \ldots, \quad n!+n$$

is a string of $n-1$ composite numbers. Why are these numbers all composite!? □

Comment. Notice, however, how very large (compared to the gap) the numbers brought up in the proof are!

4 Diophantine equations

Diophantine equations are usual equations but we are only interested in integer solutions.

Example 34. Find the general solution to the diophantine equation $16x+25y=0$.

Solution. The non-diophantine equation $16x+25y=0$ has general solution $(x,y)=(25t,-16t)$ where the parameter t is any real number.

We need to figure out for which t this results in a solution where both coordinates $x=25t$ and $y=-16t$ are integers. Obviously, t needs to be a rational number. Since $\gcd(16,25)=1$ the denominator of t must be 1, so that t must be an integer. In other words, the general solution to the diophantine equation $16x+25y=0$ is $(x,y)=(25t,-16t)$ where the parameter t is any integer.

Example 35. Find a solution to the diophantine equation $16x+25y=1$.

Solution. Since $\gcd(16,25)=1$, Bezout's theorem guarantees a solution, which we can find using the generalized Euclidean algorithm. Namely, in Example 15, we found that $-7\cdot 25+11\cdot 16=1$.

In other words, we have found the solution $x=11$ and $y=-7$. In short, $\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 11 \\ -7 \end{bmatrix}$.

Are there other solutions? **Yes!** For instance, $x=-14$ and $y=9$.

What is the **general solution**?

Solution. In the previous example we determined that the general solution to the corresponding **homogeneous (diophantine) equation** $16x+25y=0$ is $\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 25 \\ -16 \end{bmatrix}t$ where the parameter t is any integer.

We can add these solutions to any **particular solution** of $16x+25y=1$ to obtain the general solution to $16x+25y=1$. Therefore, the general solution is

$$\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 11 \\ -7 \end{bmatrix}+\begin{bmatrix} 25 \\ -16 \end{bmatrix}t=\begin{bmatrix} 11+25t \\ -7-16t \end{bmatrix},$$

where t is any integer.

Comment. Note that $t=-1$ results in $\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 11-25 \\ -7+16 \end{bmatrix}=\begin{bmatrix} -14 \\ 9 \end{bmatrix}$, another solution that we observed earlier.

Example 36. Find the general solution to the diophantine equation $16x+25y=3$.

Solution. It follows from the previous example that a particular solution is $\begin{bmatrix} x \\ y \end{bmatrix}=3\begin{bmatrix} 11 \\ -7 \end{bmatrix}$.

Hence, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 33 \\ -21 \end{bmatrix}+\begin{bmatrix} 25 \\ -16 \end{bmatrix}t=\begin{bmatrix} 33+25t \\ -21-16t \end{bmatrix}$.

Example 37. Find the general solution to the diophantine equation $6x+15y=10$.

Solution. This equation has no (integer) solution because the left-hand side is divisible by $\gcd(6,15)=3$ but the right-hand side is not divisible by 3.

Armin Straub
straub@southalabama.edu

Lemma 38. Let $a, b \in \mathbb{Z}$ (not both zero). The diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$.

Proof.
"$\Longrightarrow$" (the "only if" part): Let $d = \gcd(a, b)$. Then d divides $ax + by$. This implies that $d|c$.
"$\Longleftarrow$" (the "if" part): This is a consequence of Bezout's identity. □

Note that we can therefore focus on diophantine equations $ax + by = c$ with $\gcd(a, b) = 1$.

(Otherwise, just divide both sides by $\gcd(a, b)$.)

Theorem 39. The diophantine equation $ax + by = c$ with $\gcd(a, b) = 1$ has the general solution

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + \begin{bmatrix} b \\ -a \end{bmatrix} t,$$

where $t \in \mathbb{Z}$ is a parameter, and x_0, y_0 is any particular solution.

How to find a particular solution? Since $\gcd(a, b) = 1$, we can find integers x_1, y_1 such that $ax_1 + by_1 = 1$ (this is Bezout's identity). Multiply both sides with c, to see that we can take $x_0 = cx_1$ and $y_0 = cy_1$.

Proof. First, let us consider the case of all real solutions. The general solution of $ax + by = c$ (which describes a line!) can be described as $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + \begin{bmatrix} b \\ -a \end{bmatrix} t$.

Since $\gcd(a, b) = 1$, this solution will be integers if and only if t is an integer. □

Example 40. $56x + 72y = 2$ has no integer solutions (because $8|(56x + 72y)$ but $8 \nmid 2$).

Example 41. Find the general solution to the diophantine equation $56x + 72y = 24$.

Solution. We first note that this equation has an integer solution because 24 is a multiple of $\gcd(56, 72) = 8$.
To make our life easier, and to apply the theorem, we divide by 8 to get the equivalent equation $7x + 9y = 3$.
A solution to $7x + 9y = 1$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix}$ (and we can always find such a solution using the Euclidean algorithm).
Therefore, a solution to $7x + 9y = 3$ is $\begin{bmatrix} x \\ y \end{bmatrix} = 3 \cdot \begin{bmatrix} 4 \\ -3 \end{bmatrix} = \begin{bmatrix} 12 \\ -9 \end{bmatrix}$.
In conclusion, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 12 \\ -9 \end{bmatrix} + \begin{bmatrix} 9 \\ -7 \end{bmatrix} t$.
Caution. Why would it be incorrect to state the general solution as $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 12 \\ -9 \end{bmatrix} + \begin{bmatrix} 72 \\ -56 \end{bmatrix} t$ for $t \in \mathbb{Z}$?

Example 42. (review)

- $56x+72y=15$ has no integer solutions (because the left side is even but the right side is odd).
- $56x+72y=2$ has no integer solutions (because $8|(56x+72y)$ but $8\nmid 2$).
- $56x+72y=8$ has an integer solution (that's Bezout's identity!) and we can find it using the Euclidean algorithm ($\gcd(56,72)=8$).

  To make our life easier, we divide by 8 to get the equivalent equation $7x+9y=1$.
  One solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix}$, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix} + \begin{bmatrix} 9 \\ -7 \end{bmatrix} t$ where $t \in \mathbb{Z}$.
- $56x+72y=k$ has an integer solution if and only if k is a multiple of $\gcd(56,72)=8$.
- Determine all solutions to the diophantine equation $56x+72y=40$.

  Solution. We divide by $\gcd(56,72)=8$ to get $7x+9y=5$.
  As observed above (or by using the Euclidean algorithm), a solution to $7x+9y=1$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix}$.
  Hence, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = 5\begin{bmatrix} 4 \\ -3 \end{bmatrix} + \begin{bmatrix} 9 \\ -7 \end{bmatrix} t$ where $t \in \mathbb{Z}$.

Example 43. (problem of the "hundred fowls", appears in Chinese textbooks from the 6th century) If a rooster is worth five coins, a hen three coins, and three chicks together one coin, how many roosters, hens, and chicks, totaling 100, can be bought for 100 coins?

Solution. Let x be the number of roosters, y be the number of hens, z be the number of chicks.

$$\begin{aligned} x+y+z &= 100 \\ 5x+3y+\frac{1}{3}z &= 100 \end{aligned}$$

Eliminating z from the equations by taking $3\mathrm{eq}_2 - \mathrm{eq}_1$, we get $14x+8y=200$, or, $7x+4y=100$.

- Since 100 is a multiple of $\gcd(7,4)=1$, this equation does have integer solutions.
- We see (or find using the Euclidean algorithm) that a solution to $7x+4y=1$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$.
- Hence, $7x+4y=100$ has general solution $\begin{bmatrix} x \\ y \end{bmatrix} = 100\begin{bmatrix} -1 \\ 2 \end{bmatrix} + \begin{bmatrix} 4 \\ -7 \end{bmatrix} t = \begin{bmatrix} -100+4t \\ 200-7t \end{bmatrix}$ where $t \in \mathbb{Z}$.
- We can find z using one of the original equations: $z = 100-x-y = 3t$.
- We are only interested in solutions with $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$.
  $x \geqslant 0$ means $t \geqslant 25$. $y \geqslant 0$ means $t \leqslant 28+\frac{4}{7}$. $z \geqslant 0$ means $t \geqslant 0$.
- Hence, $t \in \{25,26,27,28\}$.
  The four corresponding solutions (x,y,z) are $(0,25,75)$, $(4,18,78)$, $(8,11,81)$, $(12,4,84)$.

Armin Straub
straub@southalabama.edu

Solving diophantine equations can be incredibly hard!

Example 44. You may have seen Pythagorean triples, which are solutions to the diophantine equation $x^2+y^2=z^2$.

A few cases. Some solutions (x,y,z) are $(3,4,5)$, $(6,8,10)$ (boring! why?!), $(5,12,13)$, $(8,15,17)$, ...

The general solution. $(m^2-n^2, 2mn, m^2+n^2)$ is a Pythagorean triple for any integers m,n.

These solutions plus scaling generate all Pythagorean triples!

For instance, $m=2, n=1$ produces $(3,4,5)$, while $m=3, n=2$ produces $(5,12,13)$.

Fermat's last theorem. For, $n>2$, the diophantine equation $x^n+y^n=z^n$ has no solutions!

Pierre de Fermat (1637) claimed in a margin of Diophantus' book *Arithmetica* that he had a proof ("I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.").

It was finally proved by Andrew Wiles in 1995 (using a connection to modular forms and elliptic curves).

This problem is often reported as the one with the largest number of unsuccessful proofs.

Example 45. (HW) Determine all solutions of $4x+7y=67$ with x and y positive integers.

Solution. We see that $x=2$, $y=-1$ is a solution to $4x+7y=1$ (you can, of course, use the Euclidean algorithm if you wish).

Hence, a particular solution to $4x+7y=67$ is given by $x=134$, $y=-67$.

The general solution to $4x+7y=67$ is thus given by $x=134+7t$, $y=-67-4t$, where t can be any integer.

- $x>0$ if and only if $134+7t>0$ if and only if $t>-\frac{134}{7}\approx -19.14$. That is, $t=-19,-18,\ldots$
- $y>0$ if and only if $-67-4t>0$ if and only if $t<-\frac{67}{4}=-16.75$. That is, $t=-17,-18,\ldots$

Hence, we get a solution (x,y) with positive integers x, y for $t=-19,-18,-17$. The three corresponding solutions are: $(1,9)$, $(8,5)$, $(15,1)$.

5 Congruences

Example 46. Today is Tuesday. What day of the week will it be a year (365 days) from now?

Solution. Since $365\equiv 1 \pmod 7$, it will be Wednesday (on 9/1/2021).

$$a\equiv b \pmod n \qquad \text{means} \qquad a=b+mn \quad (\text{for some } m\in\mathbb{Z})$$

In that case, we say that "a is congruent to b modulo n".

- In other words: $a\equiv b \pmod n$ if and only if $a-b$ is divisible by n.
- In yet other words: $a\equiv b \pmod n$ if and only if a and b leave the same remainder when dividing by n.

Example 47. $17\equiv 5 \pmod{12}$ as well as $17\equiv 29\equiv -7 \pmod{12}$

Example 48. We will discuss in more detail that, and how, we can calculate with congruences. Here is an appetizer: What is 2^{100} modulo 3? That is, what's the remainder upon division by 3?

Solution. $2\equiv -1 \pmod 3$. Hence, $2^{100}\equiv (-1)^{100}=1 \pmod 3$.

Theorem 49. We can calculate with congruences.

- First of all, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

  In other words, being congruent is a **transitive property**.
  Why? $n|(b-a)$ and $n|(c-b)$, then $n|\underbrace{((b-a)+(c-b))}_{=c-a}$.
  Alternatively, we can note that each of a, b, c leaves the same remainder when dividing by n.

- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

  (a) $a+c \equiv b+d \pmod{n}$

  Why? $(b+d)-(a+c)=(b-a)+(d-c)$ is indeed divisible by n
  (because $n|(b-a)$ and $n|(d-c)$).

  (b) $ac \equiv bd \pmod{n}$

  Why? $bd-ac=(bd-bc)+(bc-ac)=b(d-c)+c(b-a)$ is indeed divisible by n
  (because $n|(b-a)$ and $n|(d-c)$).

- In particular, if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Example 50. Compute $36 \cdot 75 \pmod{11}$.

Solution. Since $36 \equiv 3 \pmod{11}$ and $75 \equiv -2 \pmod{11}$, we have $36 \cdot 75 \equiv 3 \cdot (-2) = -6 \equiv 5 \pmod{11}$.
Important comment. We do not need to compute that $36 \cdot 75 = 2700$ (and then reduce modulo 11)! Our ability to avoid computing large intermediate quantities is crucial for applications like cryptography.

Example 51. Show that $41|2^{20}-1$.

Solution. In other words, we need to show that $2^{20}\equiv 1 \pmod{41}$.
$2^5=32\equiv -9 \pmod{41}$. Hence, $2^{20}=(2^5)^4\equiv(-9)^4=81^2\equiv(-1)^2=1 \pmod{41}$.

We saw last time that we can calculate with congruences. However:

Example 52. (caution!) If $a\equiv b \pmod{n}$, then $ac\equiv bc \pmod{n}$ for any integer c.
However, the converse is not true! We can have $ac\equiv bc \pmod{n}$ without $a\equiv b \pmod{n}$ (even assuming that $c\not\equiv 0$).

For instance. $2\cdot 4\equiv 2\cdot 1 \pmod{6}$ but $4\not\equiv 1 \pmod{6}$
However. $2\cdot 4\equiv 2\cdot 1 \pmod{6}$ means $2\cdot 4=2\cdot 1+6m$. Hence, $4=1+3m$, or, $4\equiv 1 \pmod{3}$.

Similarly, $ab\equiv 0 \pmod{n}$ does not always imply that $a\equiv 0 \pmod{n}$ or $b\equiv 0 \pmod{n}$.

For instance. $4\cdot 15\equiv 0 \pmod{6}$ but $4\not\equiv 0 \pmod{6}$ and $15\not\equiv 0 \pmod{6}$

These issues do not occur when n is a prime, as the next results shows.

Lemma 53. Let p be a prime.

(a) If $ab\equiv 0 \pmod{p}$, then $a\equiv 0 \pmod{p}$ or $b\equiv 0 \pmod{p}$.

(b) Suppose $c\not\equiv 0 \pmod{p}$. If $ac\equiv bc \pmod{p}$, then $a\equiv b \pmod{p}$.

Proof.

(a) This statement is equivalent to Lemma 19: if $p|ab$ then $p|a$ or $p|b$.

(b) $ac\equiv bc \pmod{p}$ means that p divides $ac-bc=(a-b)c$.
Since p is a prime, it follows that $p|(a-b)$ or $p|c$.
In the latter case, $c\equiv 0 \pmod{p}$, which we excluded. Hence, $p|(a-b)$. That is, $a\equiv b \pmod{p}$. □

5.1 Congruences: modular inverses

We saw that $ac\equiv bc \pmod{n}$ does not always imply $a\equiv b \pmod{n}$.
For instance, $2\cdot 4\equiv 2\cdot 1 \pmod{6}$ but $4\not\equiv 1 \pmod{6}$.
The reason is that 2 is not invertible modulo 6.

The issue is that $2|6$ which results in $2\cdot 3\equiv 0 \pmod{6}$.

Let us briefly discuss residues that are invertible modulo n.

Example 54. Note that $3\cdot 7\equiv 1 \pmod{10}$. Hence, we write $3^{-1}\equiv 7 \pmod{10}$ and say that 7 is the **modular inverse** of 3 modulo 10.

Comment. As expected, we have $(x^{-1})^{-1}\equiv x \pmod{n}$. Here, $(3^{-1})^{-1}\equiv 7^{-1}\equiv 3 \pmod{10}$.

Example 55. Solve $3x\equiv 4 \pmod{10}$.

Solution. From the previous problem, we know that $3^{-1}\equiv 7 \pmod{10}$.
Hence, $x\equiv 3^{-1}\cdot 4\equiv 7\cdot 4=8 \pmod{10}$.

Armin Straub
straub@southalabama.edu

Example 56. Determine $4^{-1} \pmod{13}$.

Brute force solution. We need to find a residue x such that $4x \equiv 1 \pmod{13}$. We can try the values $0, 1, 2, 3, \ldots, 12$ and find that $x = 10$ is the only solution modulo 13 (because $4 \cdot 10 \equiv 1 \pmod{13}$).

This approach may be fine for small examples when working by hand, but is not practical for serious congruences. On the other hand, the Euclidean algorithm can compute modular inverses extremely efficiently (see below).

Glancing. In this special case, we can actually see the solution if we notice that $4 \cdot 3 = 12$, so that $4 \cdot 3 \equiv -1 \pmod{13}$ and therefore $4^{-1} \equiv -3 \pmod{13}$. [Or, equivalently, $-4^{-1} \equiv 10 \pmod{13}$.]

Solution. Since $\gcd(4, 13) = 1$, Bézout's identity promises that $4r + 13s = 1$ for some integers r, s. Reducing $4r + 13s = 1$ modulo 13, we find $4r \equiv 1 \pmod{13}$, so that $4^{-1} \equiv r \pmod{13}$.

Using the Euclidean algorithm, we find, for instance, $r = 10$ and $s = -3$. Hence, $4^{-1} \equiv 10 \pmod{13}$.

Example 57. Solve $4x \equiv 5 \pmod{13}$.

Solution. From the previous problem, we know that $4^{-1} \equiv -3 \pmod{13}$.

Hence, $x \equiv 4^{-1} \cdot 5 \equiv -3 \cdot 5 = -2 \pmod{13}$.

Advanced comment. We were able to solve $4x \equiv 5 \pmod{13}$ by computing 4^{-1} using the Euclidean algorithm instead of relying on brute force. However, for more complicated equations like $4^x \equiv 5 \pmod{13}$, we don't know any method of finding solutions x that is significantly better than brute force. Indeed, certain cryptographic methods depend precisely on the difficulty of solving congruences like $4^x \equiv 5 \pmod{13}$.

[Such a congruence is called a **discrete logarithm problem** because the solution to $4^x = 5$ is $x = \log_4(5)$.]

Example 58. Determine $16^{-1} \pmod{25}$.

Solution. Using the Euclidean algorithm, in Example 15, we found that $11 \cdot 16 - 7 \cdot 25 = 1$.

Reducing that modulo 25, we get $11 \cdot 16 \equiv 1 \pmod{25}$.

Hence, $16^{-1} \equiv 11 \pmod{25}$.

Let $a, b \in \mathbb{Z}$, not both zero. Recall that the diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$. In particular, $ax + by = 1$ has a solution if and only if $\gcd(a, b) = 1$.

Lemma 59. a is invertible modulo n if and only if $\gcd(a, n) = 1$.

Proof. The congruence $ax \equiv 1 \pmod{n}$ is equivalent to $ax + ny = 1$ where y is some integer. Note that $ax + ny = 1$ is a diophantine equation (we are looking for integer solutions x, y) and that it has a solution if and only if $\gcd(a, n) = 1$. □

Corollary 60. Let p be a prime. Then all nonzero residues are invertible modulo p.

Advanced comment. It is common to write $\mathbb{Z}/n\mathbb{Z}$ for the set of all residues modulo n. The fact that we can add and multiply as usual, makes $\mathbb{Z}/n\mathbb{Z}$ into a (finite) **ring**.

Let p be a prime. The fact that, in addition, all nonzero residues are invertible makes $\mathbb{Z}/p\mathbb{Z}$ into a (finite) **field**. The fields we are familiar with, such as $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers) are all infinite.