CMSC/Math 456: Cryptography (Fall 2022)

Lecture 9

Daniel Gottesman

Administrative

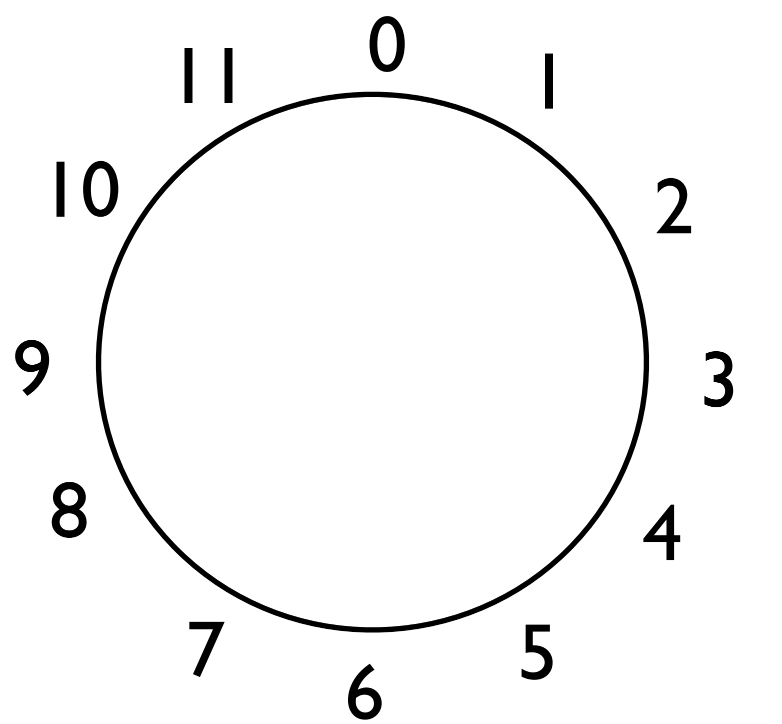
Reminder: Problem Set #4 is due Thursday (Sep. 28) at noon.

There was a typo in problem 2b (now fixed): $G_k(x)$ should be $F_k(x)$.

I apologize that I forgot to record the last lecture, but the slides are available on the public course website.

Modular Arithmetic

Modular arithmetic involves number systems that are cyclic, like a clock. Numbers mod N can be thought of as a new type of number, and type conversion between the integers and mod N arithmetic makes addition, subtraction, and multiplication obey the usual integers properties.



However, we saw that division by a is only well-defined in mod N arithmetic when gcd(a,N) = 1.

We can find the multiplicative inverse 1/a mod N by using Euclid's algorithm to find X and Y such that

$$aX + NY = \gcd(a, N)$$

Then $X = 1/a \bmod N$.

This class is being recorded

Euclid's Algorithm

Given a and b, Euclid's algorithm finds X and Y such that

$$aX + bY = \gcd(a, b)$$

- The basic idea of the algorithm is to keep a pair a_i and b_i which have the same gcd.
- At each step, we subtract off multiples of the smaller member of the pair in order to get a new pair.
- Each time we do this, we keep track of what multiple is subtracted in order to write $a_i = aX_i + bY_i$ and $b_i = aX'_i + bY'_i$.
- We combine the pair into even and odd elements of a single sequence r_i.

Euclid's Algorithm

Let $r_0 = a$ and $r_1 = b$. Assume $a > b$.

$i = 1, X_0 = 1, Y_0 = 0, X_1 = 0, Y_1 = 1$

Repeat:

$r_{i+1} = r_{i-1} \bmod r_i$

$m_i = \lfloor r_{i-1}/r_i \rfloor$

$X_{i+1} = X_{i-1} - m_i X_i$

$Y_{i+1} = Y_{i-1} - m_i Y_i$

$i = i + 1$

Until $r_i = 0$

Output:

$\gcd(a, b) = r_{i-1}$

$X = X_{i-1}, Y = Y_{i-1}$

Example:

$r_0 = 57, r_1 = 22$

$r_2 = 13,$
$X_2 = 1, Y_2 = -2$

$r_3 = 9,$
$X_3 = -1, Y_3 = 3$

$r_4 = 4,$
$X_4 = 2, Y_4 = -5$

$r_5 = 1,$
$X_5 = -5, Y_5 = 13$

$r_6 = 0$

$\gcd(57,22) = 1,$
$1 = -5 \cdot 57 + 13 \cdot 22$

Euclid’s Algorithm Analysis

Claim: At every iteration of the algorithm, the following statements are true:

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

We are going to prove this claim by induction.

We can first check the base cases i=0,1:

This class is being recorded

Euclid’s Algorithm Analysis

Claim: At every iteration of the algorithm, the following statements are true:

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

We are going to prove this claim by induction.

We can first check the base cases i=0,1:

- A: $0 \leq r_1 = b < r_0 = a$

Euclid's Algorithm Analysis

Claim: At every iteration of the algorithm, the following statements are true:

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

We are going to prove this claim by induction.

We can first check the base cases i=0,1:

- A: $0 \leq r_1 = b < r_0 = a$
- B: $r_0 = aX_0 + bY_0 = a \cdot 1 + b \cdot 0$

Euclid's Algorithm Analysis

Claim: At every iteration of the algorithm, the following statements are true:

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

We are going to prove this claim by induction.

We can first check the base cases i=0,1:

- A: $0 \leq r_1 = b < r_0 = a$
- B: $r_0 = aX_0 + bY_0 = a \cdot 1 + b \cdot 0$
- B: $r_1 = aX_1 + bY_1 = a \cdot 0 + b \cdot 1$

Euclid's Algorithm Analysis

Claim: At every iteration of the algorithm, the following statements are true:

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

We are going to prove this claim by induction.

We can first check the base cases i=0,1:

- A: $0 \leq r_1 = b < r_0 = a$
- B: $r_0 = aX_0 + bY_0 = a \cdot 1 + b \cdot 0$
- B: $r_1 = aX_1 + bY_1 = a \cdot 0 + b \cdot 1$
- C: $\gcd(a, b) \mid r_0 = a$ and $\gcd(a, b) \mid r_1 = b$

Euclid's Algorithm Analysis

We now need to prove the inductive step: Suppose we have

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

and

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$m_i = \lfloor r_{i-1} / r_i \rfloor$$

$$X_{i+1} = X_{i-1} - m_i X_i$$

$$Y_{i+1} = Y_{i-1} - m_i Y_i$$

Then

Euclid's Algorithm Analysis

We now need to prove the inductive step: Suppose we have

A. $0 \le r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

and

$$r_{i+1} = r_{i-1} \bmod r_i$$
$$m_i = \lfloor r_{i-1}/r_i \rfloor$$
$$X_{i+1} = X_{i-1} - m_i X_i$$
$$Y_{i+1} = Y_{i-1} - m_i Y_i$$

Then

- A: $0 \le r_{i+1} < r_i$ by the properties of mod

Euclid's Algorithm Analysis

We now need to prove the inductive step: Suppose we have

A. $0 \leq r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

and

$$r_{i+1} = r_{i-1} \bmod r_i$$
$$m_i = \lfloor r_{i-1} / r_i \rfloor$$
$$X_{i+1} = X_{i-1} - m_i X_i$$
$$Y_{i+1} = Y_{i-1} - m_i Y_i$$

Then

- A: $0 \leq r_{i+1} < r_i$ by the properties of mod
- C: $r_{i+1} = r_{i-1} - m_i r_i$, and since $\gcd(a, b)$ divides both terms on the RHS, $\gcd(a, b) \mid r_{i+1}$

Euclid's Algorithm Analysis

We now need to prove the inductive step: Suppose we have

A. $0 \le r_i < r_{i-1}$

B. $r_i = aX_i + bY_i$

C. $\gcd(a, b) \mid r_i$

and

$$r_{i+1} = r_{i-1} \bmod r_i$$
$$m_i = \lfloor r_{i-1}/r_i \rfloor$$
$$X_{i+1} = X_{i-1} - m_i X_i$$
$$Y_{i+1} = Y_{i-1} - m_i Y_i$$

Then

- A: $0 \le r_{i+1} < r_i$ by the properties of mod
- C: $r_{i+1} = r_{i-1} - m_i r_i$, and since $\gcd(a, b)$ divides both terms on the RHS, $\gcd(a, b) \mid r_{i+1}$
- and B:

$$\begin{aligned} aX_{i+1} + bY_{i+1} &= a(X_{i-1} - m_i X_i) + b(Y_{i-1} - m_i Y_i) \\ &= (aX_{i-1} + bY_{i-1}) - m_i(aX_i + bY_i) \\ &= r_{i-1} - m_i r_i \\ &= r_{i+1} \end{aligned}$$

Euclid's Algorithm Analysis

Thus, these three properties hold true for all i.

$$0 \leq r_i < r_{i-1}$$

$$r_i = aX_i + bY_i$$

$$\gcd(a, b) \mid r_i$$

Euclid’s Algorithm Analysis

Thus, these three properties hold true for all i.

$$0 \le r_i < r_{i-1}$$

$$r_i = aX_i + bY_i$$

$$\gcd(a, b) \mid r_i$$

- Since r_i strictly decreases, the algorithm must eventually reach $r_i = 0$, at which point it terminates with $i - 1 = i_f$.

Euclid's Algorithm Analysis

Thus, these three properties hold true for all i.

$$0 \le r_i < r_{i-1}$$

$$r_i = aX_i + bY_i$$

$$\gcd(a, b) \mid r_i$$

- Since r_i strictly decreases, the algorithm must eventually reach $r_i = 0$, at which point it terminates with $i - 1 = i_f$.
- At that point, $r_{i_f} \mid r_{i_f-1}$ since $0 = r_{i_f+1} = r_{i_f-1} - m_{i_f} r_{i_f}$.

Euclid's Algorithm Analysis

Thus, these three properties hold true for all i.

$$0 \le r_i < r_{i-1}$$

$$r_i = aX_i + bY_i$$

$$\gcd(a, b) \mid r_i$$

- Since r_i strictly decreases, the algorithm must eventually reach $r_i = 0$, at which point it terminates with $i - 1 = i_f$.
- At that point, $r_{i_f} \mid r_{i_f - 1}$ since $0 = r_{i_f+1} = r_{i_f-1} - m_{i_f} r_{i_f}$.
- But that means $r_{i_f} \mid r_{i_f-2} = m_{i_f-1} r_{i_f-1} + r_{i_f}$ and so on. By induction, we also have $r_{i_f} \mid r_j$ for all j.

Euclid's Algorithm Analysis

Thus, these three properties hold true for all i.

$$0 \le r_i < r_{i-1}$$

$$r_i = aX_i + bY_i$$

$$\gcd(a,b) \mid r_i$$

- Since r_i strictly decreases, the algorithm must eventually reach $r_i = 0$, at which point it terminates with $i - 1 = i_f$.
- At that point, $r_{i_f} \mid r_{i_f-1}$ since $0 = r_{i_f+1} = r_{i_f-1} - m_{i_f} r_{i_f}$.
- But that means $r_{i_f} \mid r_{i_f-2} = m_{i_f-1} r_{i_f-1} + r_{i_f}$ and so on. By induction, we also have $r_{i_f} \mid r_j$ for all j.
- In particular, $r_{i_f} \mid a$ and $r_{i_f} \mid b$, so $r_{i_f} \le \gcd(a,b)$.

Euclid's Algorithm Analysis

Thus, these three properties hold true for all i.

$$0 \leq r_i < r_{i-1}$$

$$r_i = aX_i + bY_i$$

$$\gcd(a, b) \mid r_i$$

- Since r_i strictly decreases, the algorithm must eventually reach $r_i = 0$, at which point it terminates with $i - 1 = i_f$.
- At that point, $r_{i_f} \mid r_{i_f-1}$ since $0 = r_{i_f+1} = r_{i_f-1} - m_{i_f} r_{i_f}$.
- But that means $r_{i_f} \mid r_{i_f-2} = m_{i_f-1} r_{i_f-1} + r_{i_f}$ and so on. By induction, we also have $r_{i_f} \mid r_j$ for all j.
- In particular, $r_{i_f} \mid a$ and $r_{i_f} \mid b$, so $r_{i_f} \leq \gcd(a, b)$.
- But $\gcd(a, b) \mid r_{i_f}$, so

$$r_{i_f} = aX_{i_f} + bY_{i_f} = \gcd(a, b)$$

Efficiency of Euclid's Algorithm

How quickly does r_i decrease in Euclid's algorithm?

If $r_i \geq r_{i-1}/2$, then $r_{i+1} \leq r_{i-1}/2$.

If $r_i \leq r_{i-1}/2$, then $r_{i+1} \leq r_i \leq r_{i-1}/2$.

Either way, $r_{i+1} \leq r_{i-1}/2$.

Since r_i is at least halved every 2 steps, the algorithm can run at most $2 \log_2 a$ steps before halting.

Meaning of Efficient

It's important to remember that efficient (or polynomial time) means polynomial time as a function of the input size.

When doing arithmetic or finding the gcd, the input size is the length (i.e., number of bits) of the numbers being computed with.

Not polynomial in the numbers themselves!

Integer addition, subtraction, multiplication, division (with remainder) are all efficient in this sense using standard grade school algorithms. Still true for modular +, -, *.

$\log_2 a$ is the input size, so Euclid's algorithm has a polynomial number of steps, each of which is efficient. Therefore it is efficient overall.

Prime vs. Non-Prime Moduli

Because division mod N is well-defined only when $\gcd(a, N) = 1$, there is an important difference in structure between values of N with many factors (so there are few numbers which are relatively prime to it) and those with few factors (so most numbers are relatively prime to N).

In particular, when N is prime, we can divide by *any* number mod N except for 0.

In mathematical jargon, numbers mod N form a field when N is prime, whereas they are only a ring when N is not prime.

(You don't need to know these terms; the thing you should understand is why prime N is different and special.)

Modular Arithmetic Examples

Mod 5 addition and multiplication:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Each non-zero row and column has all #s

Mod 6 addition and multiplication:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Rows and columns have 0s and repeat #s

This class is being recorded

Exponentiation

The next operation we need in modular arithmetic, and one we will use a lot, is exponentiation:

$$x^a \bmod N$$

Here, x is a number mod N, and a is an integer. (We will see later that we can safely restrict the range of a but it is *not* a mod N number.)

Exponentiation is defined in the usual way, as the product of a copies of x, with multiplication defined in mod N arithmetic.

Many of the usual properties of exponents hold, e.g.:

$$x^a x^b = x^{a+b} \bmod N$$

$$(x^a)^b = x^{ab} \bmod N$$

$$x^a y^a = (xy)^a \bmod N$$

Example: Mod 10

Let us calculate exponents mod 10.

$0^1 = 0 \bmod 10$

$1^1 = 1 \bmod 10$

$4^1 = 4 \bmod 10$
$4^2 = 6 \bmod 10$

$5^1 = 5 \bmod 10$

$6^1 = 6 \bmod 10$

$9^1 = 9 \bmod 10$
$9^2 = 1 \bmod 10$

$2^1 = 2 \bmod 10$
$2^2 = 4 \bmod 10$
$2^3 = 8 \bmod 10$
$2^4 = 6 \bmod 10$

$8^1 = 8 \bmod 10$
$8^2 = 4 \bmod 10$
$8^3 = 2 \bmod 10$
$8^4 = 6 \bmod 10$

$3^1 = 3 \bmod 10$
$3^2 = 9 \bmod 10$
$3^3 = 7 \bmod 10$
$3^4 = 1 \bmod 10$

$7^1 = 7 \bmod 10$
$7^2 = 9 \bmod 10$
$7^3 = 3 \bmod 10$
$7^4 = 1 \bmod 10$

Notice that the powers start to repeat after this point. Then they cycle.

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$$3^1 = 3 \bmod 10$$
$$3^2 = 9 \bmod 10$$
$$3^3 = 7 \bmod 10$$
$$3^4 = 1 \bmod 10$$

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$3^1 = 3 \bmod 10$

$3^2 = 9 \bmod 10$

$3^3 = 7 \bmod 10$

$3^4 = 1 \bmod 10$

Remember, we can reduce mod N before or after multiplying and get the same result:
$3^4 = 81 = 1 \bmod 10$ and
$3 \cdot 7 = 21 = 1 \bmod 10$

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$3^1 = 3 \bmod 10$

$3^2 = 9 \bmod 10$

$3^3 = 7 \bmod 10$

$3^4 = 1 \bmod 10$

$3^5 = 3 \bmod 10$

Remember, we can reduce mod N before or after multiplying and get the same result: $3^4 = 81 = 1 \bmod 10$ and $3 \cdot 7 = 21 = 1 \bmod 10$

We can get $3^5 \bmod 10$ by just multiplying $3^4 = 1 \bmod 10$ by 3.

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$3^1 = 3 \bmod 10$

$3^2 = 9 \bmod 10$

$3^3 = 7 \bmod 10$

$3^4 = 1 \bmod 10$

$3^5 = 3 \bmod 10$

$3^6 = 9 \bmod 10$

$3^7 = 7 \bmod 10$

$3^8 = 1 \bmod 10$

Remember, we can reduce mod N before or after multiplying and get the same result:
$3^4 = 81 = 1 \bmod 10$ and
$3 \cdot 7 = 21 = 1 \bmod 10$

We can get $3^5 \bmod 10$ by just multiplying $3^4 = 1 \bmod 10$ by 3.

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$3^1 = 3 \bmod 10$

$3^2 = 9 \bmod 10$

$3^3 = 7 \bmod 10$

$3^4 = 1 \bmod 10$

$3^5 = 3 \bmod 10$

$3^6 = 9 \bmod 10$

$3^7 = 7 \bmod 10$

$3^8 = 1 \bmod 10$

Remember, we can reduce mod N before or after multiplying and get the same result: $3^4 = 81 = 1 \bmod 10$ and $3 \cdot 7 = 21 = 1 \bmod 10$

We can get $3^5 \bmod 10$ by just multiplying $3^4 = 1 \bmod 10$ by 3.

Once we get back to 1, the cycle starts repeating again.

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$3^1 = 3 \bmod 10$

$3^2 = 9 \bmod 10$

$3^3 = 7 \bmod 10$

$3^4 = 1 \bmod 10$

$3^5 = 3 \bmod 10$

$3^6 = 9 \bmod 10$

$3^7 = 7 \bmod 10$

$3^8 = 1 \bmod 10$

$3^9 = 3 \bmod 10$

$\vdots$

Remember, we can reduce mod N before or after multiplying and get the same result: $3^4 = 81 = 1 \bmod 10$ and $3 \cdot 7 = 21 = 1 \bmod 10$

We can get $3^5 \bmod 10$ by just multiplying $3^4 = 1 \bmod 10$ by 3.

Once we get back to 1, the cycle starts repeating again.

Powers Form a Cycle

To see how the cycling works, let's look at powers of 3 mod 10.

$3^1 = 3 \bmod 10$

$3^2 = 9 \bmod 10$

$3^3 = 7 \bmod 10$

$3^4 = 1 \bmod 10$

$3^5 = 3 \bmod 10$

$3^6 = 9 \bmod 10$

$3^7 = 7 \bmod 10$

$3^8 = 1 \bmod 10$

$3^9 = 3 \bmod 10$

$\vdots$

Remember, we can reduce mod N before or after multiplying and get the same result: $3^4 = 81 = 1 \bmod 10$ and $3 \cdot 7 = 21 = 1 \bmod 10$

We can get $3^5 \bmod 10$ by just multiplying $3^4 = 1 \bmod 10$ by 3.

Once we get back to 1, the cycle starts repeating again.

Powers of 3 mod 10 repeat in a cycle of length 4.

Repetition of Powers

Since there are only N possible values mod N, eventually x^a must repeat, $x^{r+1} = x \bmod N$. If x and N are relatively prime, then we can cancel x and get $x^r = 1 \bmod N$.

Definition: If $\gcd(x, N) = 1$ and r is the lowest power for which $x^r = 1 \bmod N$, then r is the order of x, ord(x).

After r, powers of x start to repeat:

$$x^a = x^{\mathrm{ord}(x)} x^{a-\mathrm{ord}(x)} = 1 \cdot x^{a-\mathrm{ord}(x)} = x^{a-\mathrm{ord}(x)} \bmod N$$

Or more generally,

$$x^a = x^b \bmod N \text{ iff } a = b \bmod \mathrm{ord}(x)$$

So, for example, ord(3) = 4 in mod 10 arithmetic and

$$3^a = 3^b \bmod 10 \text{ iff } a = b \bmod 4 \Leftrightarrow a = b + 4k$$

Different Orders Mod 10

The numbers relatively prime to 10 are 1, 3, 7, and 9.

$$1^1 = 1 \bmod 10$$

ord(1) = 1

$$3^1 = 3 \bmod 10$$
$$3^2 = 9 \bmod 10$$
$$3^3 = 7 \bmod 10$$
$$3^4 = 1 \bmod 10$$

ord(3) = 4

$$7^1 = 7 \bmod 10$$
$$7^2 = 9 \bmod 10$$
$$7^3 = 3 \bmod 10$$
$$7^4 = 1 \bmod 10$$

ord(7) = 4

$$9^1 = 9 \bmod 10$$
$$9^2 = 1 \bmod 10$$

ord(9) = 2

The different bases have different orders mod 10.

Closure of Relatively Prime Elements

Another observation: when we have a base x which is relatively prime to the modulus N, then all powers of x are also relatively prime to N.

Proposition: If $\gcd(x, N) = 1$ and $y = x^a \bmod N$, then $\gcd(y, N) = 1$ as well.

$3^1 = 3 \bmod 10$
$3^2 = 9 \bmod 10$
$3^3 = 7 \bmod 10$
$3^4 = 1 \bmod 10$

Closure of Relatively Prime Elements

Another observation: when we have a base x which is relatively prime to the modulus N, then all powers of x are also relatively prime to N.

Proposition: If $\gcd(x, N) = 1$ and $y = x^a \bmod N$, then $\gcd(y, N) = 1$ as well.

$3^1 = 3 \bmod 10$
$3^2 = 9 \bmod 10$
$3^3 = 7 \bmod 10$
$3^4 = 1 \bmod 10$

Proof:

We can assume $a < r = \mathrm{ord}(x)$. Then

$$x^a x^{r-a} = x^r = 1 \bmod N$$

This class is being recorded

Closure of Relatively Prime Elements

Another observation: when we have a base x which is relatively prime to the modulus N, then all powers of x are also relatively prime to N.

$$3^1 = 3 \bmod 10$$
$$3^2 = 9 \bmod 10$$
$$3^3 = 7 \bmod 10$$
$$3^4 = 1 \bmod 10$$

Proposition: If $\gcd(x, N) = 1$ and $y = x^a \bmod N$, then $\gcd(y, N) = 1$ as well.

Proof:

We can assume $a < r = \text{ord}(x)$. Then

$$x^a x^{r-a} = x^r = 1 \bmod N$$

But this implies that x^{r-a} is the multiplicative inverse of x^a.

Closure of Relatively Prime Elements

Another observation: when we have a base x which is relatively prime to the modulus N, then all powers of x are also relatively prime to N.

Proposition: If $\gcd(x, N) = 1$ and $y = x^a \bmod N$, then $\gcd(y, N) = 1$ as well.

$3^1 = 3 \bmod 10$
$3^2 = 9 \bmod 10$
$3^3 = 7 \bmod 10$
$3^4 = 1 \bmod 10$

Proof:

We can assume $a < r = \mathrm{ord}(x)$. Then

$$x^a x^{r-a} = x^r = 1 \bmod N$$

But this implies that x^{r-a} is the multiplicative inverse of x^a.

Since $y = x^a$ has a multiplicative inverse mod N, it follows that $\gcd(y, N) = 1$.

Example: Mod 10

When $\gcd(x, N) \neq 1$, the behavior is different.

$0^1 = 0 \bmod 10$

$4^1 = 4 \bmod 10$
$4^2 = 6 \bmod 10$

$5^1 = 5 \bmod 10$

$6^1 = 6 \bmod 10$

$2^1 = 2 \bmod 10$
$2^2 = 4 \bmod 10$
$2^3 = 8 \bmod 10$
$2^4 = 6 \bmod 10$

$8^1 = 8 \bmod 10$
$8^2 = 4 \bmod 10$
$8^3 = 2 \bmod 10$
$8^4 = 6 \bmod 10$

If the base shares a factor with 10, all powers still share that factor.

The exponents still cycle, but they never reach 1.

Non-Relatively Prime Elements

When the base x is *not* relatively prime to the modulus N, the powers are not relatively prime either.

$$8^1 = 8 \bmod 10$$
$$8^2 = 4 \bmod 10$$
$$8^3 = 2 \bmod 10$$
$$8^4 = 6 \bmod 10$$

Proposition: If $b = \gcd(x, N)$ and $y = x^a \bmod N$, then $b \mid y$.

In particular, if x is not relatively prime to N, then y is not either.

Non-Relatively Prime Elements

When the base x is *not* relatively prime to the modulus N, the powers are not relatively prime either.

$8^1 = 8 \bmod 10$
$8^2 = 4 \bmod 10$
$8^3 = 2 \bmod 10$
$8^4 = 6 \bmod 10$

Proposition: If $b = \gcd(x, N)$ and $y = x^a \bmod N$, then $b \mid y$.

In particular, if x is not relatively prime to N, then y is not either.

Proof: We have that $b \mid x$ in integer arithmetic.

Non-Relatively Prime Elements

When the base x is *not* relatively prime to the modulus N, the powers are not relatively prime either.

$$8^1 = 8 \bmod 10$$
$$8^2 = 4 \bmod 10$$
$$8^3 = 2 \bmod 10$$
$$8^4 = 6 \bmod 10$$

Proposition: If $b = \gcd(x, N)$ and $y = x^a \bmod N$, then $b \mid y$.

In particular, if x is not relatively prime to N, then y is not either.

Proof: We have that $b \mid x$ in integer arithmetic.

But then $b \mid cx$ for all integer c. In particular, $b \mid x^{a-1}x = x^a$.

This class is being recorded

Non-Relatively Prime Elements

When the base x is *not* relatively prime to the modulus N, the powers are not relatively prime either.

$$8^1 = 8 \bmod 10$$
$$8^2 = 4 \bmod 10$$
$$8^3 = 2 \bmod 10$$
$$8^4 = 6 \bmod 10$$

Proposition: If $b = \gcd(x, N)$ and $y = x^a \bmod N$, then $b \mid y$.

In particular, if x is not relatively prime to N, then y is not either.

Proof: We have that $b \mid x$ in integer arithmetic.

But then $b \mid cx$ for all integer c. In particular, $b \mid x^{a-1}x = x^a$.

This is in integer arithmetic. Still in integer arithmetic,

$$y = x^a + kN$$

Non-Relatively Prime Elements

When the base x is *not* relatively prime to the modulus N, the powers are not relatively prime either.

$8^1 = 8 \bmod 10$
$8^2 = 4 \bmod 10$
$8^3 = 2 \bmod 10$
$8^4 = 6 \bmod 10$

Proposition: If $b = \gcd(x, N)$ and $y = x^a \bmod N$, then $b \mid y$.

In particular, if x is not relatively prime to N, then y is not either.

Proof: We have that $b \mid x$ in integer arithmetic.

But then $b \mid cx$ for all integer c. In particular, $b \mid x^{a-1}x = x^a$.

This is in integer arithmetic. Still in integer arithmetic,

$$y = x^a + kN$$

But $b \mid N$ as well, so since b divides both terms in the RHS sum, we have $b \mid y$.

This class is being recorded

Example: Mod 11

Mod 11: Now every x is relatively prime to 11.

$$3^1 = 3 \bmod 11$$
$$3^2 = 9 \bmod 11$$
$$3^3 = 5 \bmod 11$$
$$3^4 = 4 \bmod 11$$
$$3^5 = 1 \bmod 11$$

$$5^1 = 5 \bmod 11$$
$$5^2 = 3 \bmod 11$$
$$5^3 = 4 \bmod 11$$
$$5^4 = 9 \bmod 11$$
$$5^5 = 1 \bmod 11$$

$$10^1 = 10 \bmod 11$$
$$10^2 = 1 \bmod 11$$

$$2^1 = 2 \bmod 11$$
$$2^2 = 4 \bmod 11$$
$$2^3 = 8 \bmod 11$$
$$2^4 = 5 \bmod 11$$
$$2^5 = 10 \bmod 11$$
$$2^6 = 9 \bmod 11$$
$$2^7 = 7 \bmod 11$$
$$2^8 = 3 \bmod 11$$
$$2^9 = 6 \bmod 11$$
$$2^{10} = 1 \bmod 11$$

$$7^1 = 7 \bmod 11$$
$$7^2 = 5 \bmod 11$$
$$7^3 = 2 \bmod 11$$
$$7^4 = 3 \bmod 11$$
$$7^5 = 10 \bmod 11$$
$$7^6 = 4 \bmod 11$$
$$7^7 = 6 \bmod 11$$
$$7^8 = 9 \bmod 11$$
$$7^9 = 8 \bmod 11$$
$$7^{10} = 1 \bmod 11$$

ord (2) = ord(7) = 10

ord(3) = ord(5) = 5

ord(10) = 2

Order of Elements

More generally, we are interested in which elements have which order.

Recall that 2 has order 10 in mod 11 arithmetic.

Question 1: What is the order of $4 = 2^2 \bmod 11$?

Order of Elements

More generally, we are interested in which elements have which order.

Recall that 2 has order 10 in mod 11 arithmetic.

Question 1: What is the order of $4 = 2^2 \bmod 11$?

Answer: 5, because $4^5 = (2^2)^5 = 2^{10} = 1 \bmod 11$.

Note that the answer can't be any $r < 5$, because then we would have $4^r = (2^2)^r = 2^{2r} = 1 \bmod 11$ with $2r < 10$, which we know is not possible since the order of 2 is the smallest power of 2 that gives us 1.

Order of Elements

More generally, we are interested in which elements have which order.

Recall that 2 has order 10 in mod 11 arithmetic.

Question 1: What is the order of $4 = 2^2 \bmod 11$?

Answer: 5, because $4^5 = (2^2)^5 = 2^{10} = 1 \bmod 11$.

Note that the answer can't be any $r < 5$, because then we would have $4^r = (2^2)^r = 2^{2r} = 1 \bmod 11$ with $2r < 10$, which we know is not possible since the order of 2 is the smallest power of 2 that gives us 1.

Similarly, the order of $10 = 2^5 \bmod 11$ must be 2, which we saw on the last page.

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 2: What is the order of $8 = 2^3 \bmod 11$?

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 2: What is the order of $8 = 2^3 \bmod 11$?

Answer: 10. Certainly

$$8^{10} = (2^3)^{10} = (2^{10})^3 = 1^3 = 1 \bmod 11$$

but how do we know the order is not something smaller?

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 2: What is the order of $8 = 2^3 \bmod 11$?

Answer: 10. Certainly

$$8^{10} = (2^3)^{10} = (2^{10})^3 = 1^3 = 1 \bmod 11$$

but how do we know the order is not something smaller?

Suppose $8^r = 1 \bmod 11$. Then $2^{3r} = 1 \bmod 11$.

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 2: What is the order of $8 = 2^3 \bmod 11$?

Answer: 10. Certainly

$$8^{10} = (2^3)^{10} = (2^{10})^3 = 1^3 = 1 \bmod 11$$

but how do we know the order is not something smaller?

Suppose $8^r = 1 \bmod 11$. Then $2^{3r} = 1 \bmod 11$.

Since $2^0 = 1 = 2^{3r} \bmod 11$, then 0 and 3r differ by a multiple of the order, i.e.

$$3r = 10k$$

This class is being recorded

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 2: What is the order of $8 = 2^3 \bmod 11$?

Answer: 10. Certainly

$$8^{10} = (2^3)^{10} = (2^{10})^3 = 1^3 = 1 \bmod 11$$

but how do we know the order is not something smaller?

Suppose $8^r = 1 \bmod 11$. Then $2^{3r} = 1 \bmod 11$.

Since $2^0 = 1 = 2^{3r} \bmod 11$, then 0 and 3r differ by a multiple of the order, i.e.

$$3r = 10k$$

Since 3 is relatively prime to 10, the only way this is possible is for $10 \mid r$.

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 3: What is the order of $9 = 2^6 \bmod 11$?

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 3: What is the order of $9 = 2^6 \bmod 11$?

Answer: 5. Consider:

$$9^5 = (2^6)^5 = 2^{30} = (2^{10})^3 = 1^3 = 1 \bmod 10$$

or alternatively, $9 = 8^2 \bmod 11$ and 8 has order 10.

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 3: What is the order of $9 = 2^6 \bmod 11$?

Answer: 5. Consider:

$$9^5 = (2^6)^5 = 2^{30} = (2^{10})^3 = 1^3 = 1 \bmod 10$$

or alternatively, $9 = 8^2 \bmod 11$ and 8 has order 10.

Question 3a: How could we have known it would be 5?

Order of Elements

Again, 2 has order 10 in mod 11 arithmetic.

Question 3: What is the order of $9 = 2^6 \bmod 11$?

Answer: 5. Consider:

$$9^5 = (2^6)^5 = 2^{30} = (2^{10})^3 = 1^3 = 1 \bmod 10$$

or alternatively, $9 = 8^2 \bmod 11$ and 8 has order 10.

Question 3a: How could we have known it would be 5?

Let ord(9) = r, so

$$1 = 9^r = 2^{6r} \bmod 11$$

and 6r = 10k. Since 6 is even, gcd(6,10) = 2, and we can divide through by 2 to get $3r = 5k$.

Since we divided by the gcd, what's left is relatively prime, and we must have $5 \mid r$.

Order of Elements

Theorem: Let $\gcd(x, N) = 1$ and $y = x^a \bmod N$, and let $r = \mathrm{ord}(x)$ (in mod N arithmetic). Then

$$\mathrm{ord}(y) = \frac{r}{\gcd(a, r)}$$

Proof:

Order of Elements

Theorem: Let $\gcd(x, N) = 1$ and $y = x^a \bmod N$, and let $r = \text{ord}(x)$ (in mod N arithmetic). Then

$$\text{ord}(y) = \frac{r}{\gcd(a, r)}$$

Proof: Let $b = r/\gcd(a, r)$ and $c = a/\gcd(a, r)$. Then note that b and c are relatively prime.

Order of Elements

Theorem: Let $\gcd(x, N) = 1$ and $y = x^a \bmod N$, and let $r = \mathrm{ord}(x)$ (in mod N arithmetic). Then

$$\mathrm{ord}(y) = \frac{r}{\gcd(a, r)}$$

Proof: Let $b = r/\gcd(a, r)$ and $c = a/\gcd(a, r)$. Then note that b and c are relatively prime.

By definition, $1 = y^{\mathrm{ord}(y)} = x^{a\,\mathrm{ord}(y)} \bmod N$. Thus,

$$a\,\mathrm{ord}(y) = kr$$

Order of Elements

Theorem: Let $\gcd(x, N) = 1$ and $y = x^a \bmod N$, and let $r = \operatorname{ord}(x)$ (in mod N arithmetic). Then

$$\operatorname{ord}(y) = \frac{r}{\gcd(a, r)}$$

Proof: Let $b = r/\gcd(a, r)$ and $c = a/\gcd(a, r)$. Then note that b and c are relatively prime.

By definition, $1 = y^{\operatorname{ord}(y)} = x^{a \operatorname{ord}(y)} \bmod N$. Thus,

$$a \operatorname{ord}(y) = kr$$

Dividing through by $\gcd(a, r)$, we have

$$c \operatorname{ord}(y) = kb$$

Order of Elements

Theorem: Let $\gcd(x, N) = 1$ and $y = x^a \bmod N$, and let $r = \mathrm{ord}(x)$ (in mod N arithmetic). Then

$$\mathrm{ord}(y) = \frac{r}{\gcd(a, r)}$$

Proof: Let $b = r/\gcd(a, r)$ and $c = a/\gcd(a, r)$. Then note that b and c are relatively prime.

By definition, $1 = y^{\mathrm{ord}(y)} = x^{a\,\mathrm{ord}(y)} \bmod N$. Thus,

$$a\,\mathrm{ord}(y) = kr$$

Dividing through by $\gcd(a, r)$, we have

$$c\,\mathrm{ord}(y) = kb$$

Since b and c are relatively prime, we see that $b \mid \mathrm{ord}(y)$.

Order of Elements

Theorem: Let $\gcd(x, N) = 1$ and $y = x^a \bmod N$, and let $r = \mathrm{ord}(x)$ (in mod N arithmetic). Then

$$\mathrm{ord}(y) = \frac{r}{\gcd(a, r)}$$

Proof: Let $b = r/\gcd(a, r)$ and $c = a/\gcd(a, r)$. Then note that b and c are relatively prime.

By definition, $1 = y^{\mathrm{ord}(y)} = x^{a\,\mathrm{ord}(y)} \bmod N$. Thus,

$$a\,\mathrm{ord}(y) = kr$$

Dividing through by $\gcd(a, r)$, we have

$$c\,\mathrm{ord}(y) = kb$$

Since b and c are relatively prime, we see that $b \mid \mathrm{ord}(y)$.

But $y^b = x^{ab} = x^{cr} = (x^r)^c = 1 \bmod N$, so $\mathrm{ord}(y) \le b$. Thus, $\mathrm{ord}(y) = b$.

Modular Exponentiation Summary

We have deduced the following facts about modular exponentials:

- Modular exponentials always recur in a cycle whose size is less than the modulus N.
- Powers of x relatively prime to N are also relatively prime and powers of non-relatively prime x are also not relatively prime.
- We define ord(x) as the minimum r such that $x^r = 1 \bmod N$.
- If $x^a = x^b \bmod N$, then $b = a + k\,\mathrm{ord}(x)$.
- Once we know ord(x), we can easily compute the order of all powers of x.

Efficiency of Modular Operations

We saw that Euclid's algorithm can run in a time polynomial in the length of the numbers involved. What about other modular operations, and in particular exponentiation?

To calculate $x^a \bmod N$, we could:

- Start with $x \bmod N$.
- Multiply by x a total of a times, each time reducing mod N after the multiplication.

However, this takes a total of a multiplications, which is too many: $a = O(\exp(\log a))$.

We would like a better algorithm for modular exponentiation.

Repeated Squaring

We can get large exponents quickly by repeated squaring:

From $x^i \bmod N$, we can calculate $x^{2i} \bmod N$ using 1 multiplication by squaring it.

Doing this repeatedly gives us $x, x^2, x^4, x^8, \ldots, x^{2^c}$, with only c multiplications.

To calculate $x^a \bmod N$ for general a, first write a in binary:

$$a = a_0 2^c + a_1 2^{c-1} + \cdots + a_{c-1} 2 + a_c$$

Then $$x^a = \prod_{i=0}^{c} x^{a_{c-i} 2^i}$$

This needs $O(\log a)$ multiplications.

This class is being recorded

Example:

Calculate $65^{12} \bmod 71$:

$$65^2 = 36 \bmod 71$$

$$65^4 = 36^2 = 18 \bmod 71$$

$$65^8 = 18^2 = 40 \bmod 71$$

Then

$$\begin{aligned} 65^{12} &= 65^8 \cdot 65^4 \bmod 71 \\ &= 40 \cdot 18 \bmod 71 \\ &= 10 \bmod 71 \end{aligned}$$