Fermat's Little Theorem

Last time I mentioned the following result, which is the foundation of the "RSA cryptosystem".

☆ Fermat's Little Theorem:

Let $p \in \mathbb{Z}$ be prime. Then for all integers $n \in \mathbb{Z}$ we have

$$[n^p]_p = [n]_p .$$

"$n^p = n \mod p$". ///

Fermat claimed this theorem in 1640 but he didn't provide a proof. The first proof was given by Euler in 1736.

Euler's proof was based on

- induction
- the Binomial Theorem.

{

So these will be the next two topics in the course. But first let me show you Euler's proof [there will be a gap in it].

Euler's Proof of FLT:

Let $p \in \mathbb{Z}$ be prime and for all $n \in \mathbb{Z}$ consider the statement

"$n^p = n \mod p$".

We will show that this statement is true for all $n \geq 1$.

Base Case: First note that the statement is true for $n = 0$:

"$1^p = 1 \mod p$" ✓

Induction Step: Now fix some integer $k \geq 0$ and assume for induction that

"$k^p = k \mod p$"

is a true statement.

In this case we will prove that

"$(k+1)^p = (k+1) \mod p$"

is also a true statement. Indeed, we have

$$(k+1)^p = k^p + 1^p \mod p \qquad (?)$$

$$= k + 1 \mod p \qquad \text{base case \& assumption.}$$

This concludes the proof. //

Note how this proof depends on the technology of modular arithmetic that we developed. In more abstract language we would say

$$[(k+1)^p]_p = [k^p + 1^p]_p \qquad (?)$$

$$= [k^p]_p + [1^p]_p$$

$$= [k]_p + [1]_p$$

$$= [k+1]_p .$$

But the step (?) is still unexplained. Certainly we know that

$$(k+1)^p \neq k^p + 1^p$$

as integers. So why do we have

$$[(k+1)^p]_p = [k^p + 1^p]_p \quad ?$$

we need to investigate this.

Let a & b be any "numbers" (i.e. elements of some "commutative ring"). Then using the distributive rule gives

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) \\ &= a(a+b) + b(a+b) \\ &= a^2 + ab + ba + b^2 \\ &= a^2 + 2ab + b^2 .\end{aligned}$$

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)^2 \\ &= (a+b)(a^2 + 2ab + b^2) \\ &= a(a^2 + 2ab + b^2) + b(a^2 + 2ab + b^2)\end{aligned}$$

↓

$= a^3 + 2a^2b + ab^2 + ba^2 + 2bab + b^2$

$= a^3 + 3a^2b + 3ab^2 + b^3$.

$(a+b)^4 = (a+b)(a+b)^3$

$= a(a^3 + 3a^2b + 3ab^2 + b^3)$
$\quad + b(a^3 + 3a^2b + 3ab^2 + b^3)$

$= a^4 + 3a^3b + 3a^2b^2 + ab^3 + 0$
$+ 0 + a^3b + 3a^2b^2 + 3ab^3 + b^4$

$= (1+0)a^4 + (3+1)a^3b + (3+3)a^2b^2$

$\quad + (1+3)ab^3 + (0+1)b^4$

$= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

Is there some pattern to this?

Note that each term of $(a+b)^n$ will have the form

$$C(n,k)\, a^k b^{n-k}$$

}

where $C(n,k) \in \mathbb{Z}$ is some coefficient depending on n & k. Thus we can write

$$(a+b)^n = \sum_{k=0}^{n} C(n,k)\, a^k b^{n-k}.$$

We would like to have a formula for these "binomial coefficients" $C(n,k)$.

Why?

Because if p is prime then Euler's proof uses the fact that

$$[C(p,k)]_p = [0]_p \text{ for } k \in \{1, 2, \cdots, p-1\}$$

and we want to know why this is true.

The Binomial Theorem

Let a & b be any numbers. Last time we considered the problem of computing the expansion of

$$(a+b)^n$$

where n is a positive integer. Here are some small examples.

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2+2ab+b^2$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$$

$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4.$$

In general we see that

$$(a+b)^n = \sum_{k=0}^{n} C(n,k)\, a^k b^{n-k}$$

$\downarrow$

for some integers $C(n,k) \in \mathbb{Z}$, which we call binomial coefficients.

We observed that the binomial coefficients form a pattern called "Pascal's Triangle":

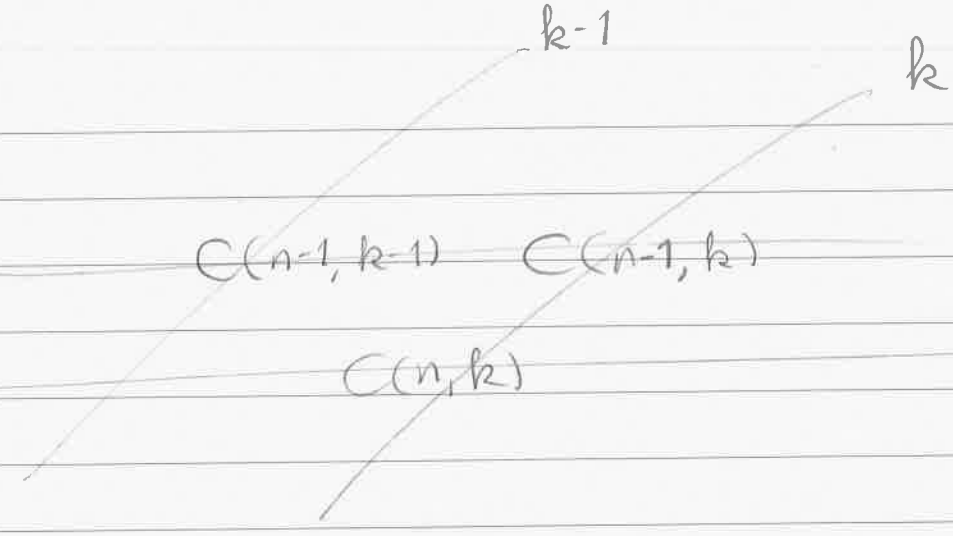
0 0 0 0 0 1 0 0 0 0 0
0 0 0 0 1 1 0 0 0 0
0 0 0 1 2 1 0 0 0
0 0 1 3 3 1 0 0
0 1 4 6 4 1 0
1 5 10 10 5 1

Here, each number is the sum of the two numbers above. Based on the picture above we predict that

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5a^1b^4 + b^5,$$

which is correct. How can we prove that this pattern holds in general?

If $C(n,k)$ is the entry in the nth row and the kth diagonal of Pascal's Triangle then the two entries above are



So we want to prove that

(*) $$C(n,k) = C(n-1, k-1) + C(n-1, k)$$

for all $n \geq 1$ and $0 \leq k \leq n$. Actually, it is convenient to define

$$C(n,k) := 0 \quad \text{when } k<0 \text{ or } k>n,$$

so that equation (*) holds for all $n \geq 1$ and for <u>all</u> $k \in \mathbb{Z}$. Then we can write

$$(a+b)^n = \sum_{k=-\infty}^{\infty} C(n,k)\, a^k b^{n-k}$$

or just $$\sum_k C(n,k)\, a^k b^{n-k}$$

and we don't have to worry about the limits of summation.

★ Theorem ("Pascal's Recurrence"): For all integers $n, k \in \mathbb{Z}$ with $n \geq 1$ we have

$$C(n,k) = C(n-1,k-1) + C(n-1,k).$$

Proof: Let a, b be any two numbers. We will express $(a+b)^n$ in two ways.

First we have

$$(a+b)^n = \sum_k C(n,k)\, a^k b^{n-k}.$$

On the other hand, we have

$$(a+b)^n = (a+b)(a+b)^{n-1}$$

$$= (a+b) \sum_k C(n-1,k)\, a^k b^{(n-1)-k}$$

$$= a \sum_k C(n-1,k)\, a^k b^{(n-1)-k} + b \sum C(n-1,k)\, a^k b^{(n-1)-k}$$

$$= \sum_k C(n-1,k)\, a^{k+1} b^{n-(k+1)} + \sum_k C(n-1,k)\, a^k b^{n-k}.$$

Then we replace $k+1$ by k in the first sum to get

$$\sum_k C(n-1, k-1)\, a^k b^{n-k} + \sum_k C(n-1, k)\, a^k b^{n-k}$$

$$= \sum_k \left[C(n-1, k-1) + C(n-1, k) \right] a^k b^{n-k}.$$

Finally, comparing coefficients in the two expressions for $(a+b)^n$ gives

$$C(n,k) = C(n-1, k-1) + C(n-1, k),$$

as desired. ///

Great. Now let's remember what we're doing. We're trying to finish Euler's proof of Fermat's little Theorem by proving that

$$[(n+1)^p]_p = [n^p]_p + [1^p]_p$$

$\{$

for all integers k and primes p.
Expanding the left side gives

$$[(n+1)^p]_p = \left[\sum_k C(p,k)\, n^k\, 1^{p-k}\right]_p$$

$$= \sum_k [C(p,k)]_p [n^k]_p [1^{p-k}]_p$$

$$= [np]_p + [1^p]_p + \underbrace{\sum_{k=1}^{p-1} [C(p,k)]_p [n^k]_p [1^{p-k}]_p}.$$

We want to prove that this sum $= [0]_p$.

In fact, we will prove the stronger statement that for all primes p we have

$$[C(p,k)]_p = [0]_p \quad \text{when } k \in \{1, 2, \ldots, p-1\}.$$

But the theorem we proved today does not immediately help with this. We really need a <u>formula</u> for the numbers

$$C(n,k).$$

☆ Definition: Given an integer $n \geq 0$ we define

$$n! := \begin{cases} n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 & \text{if } n \geq 1 \\ 1 & \text{if } n = 0 \end{cases}$$

and we call this number "n factorial".

I claim that for all relevant values of n and k we have

$$\boxed{C(n,k) = \frac{n!}{k!(n-k)!}}.$$

That's a bit out-of-the-blue. Maybe this formula is not easy to guess, but once it has been guessed it is easy to prove using Pascal's Recurrence and induction.

$\S$

For now let's just test the formula to see if it's reasonable.

Example ($n=4$):

	$C(4,k)$	$4!/(k!(4-k)!)$
$k=0$	1	$\frac{4!}{0!\,4!} = \frac{4\cdot3\cdot2\cdot1}{1\cdot4\cdot3\cdot2\cdot1} = 1$ ✓
$k=1$	4	$\frac{4!}{1!\,3!} = \frac{4\cdot3\cdot2\cdot1}{1\cdot3\cdot2\cdot1} = 4$ ✓
$k=2$	6	$\frac{4!}{2!\,2!} = \frac{{}^{2}4\cdot3\cdot2\cdot1}{2\cdot1\cdot2\cdot1} = 6$ ✓
$k=3$	4	$\frac{4!}{3!\,1!} = \frac{4\cdot3\cdot2\cdot1}{3\cdot2\cdot1\cdot1} = 4$ ✓
$k=4$	1	$\frac{4!}{4!\,0!} = \frac{4\cdot3\cdot2\cdot1}{4\cdot3\cdot2\cdot1\cdot1} = 1$ ✓

It seems to work.

Euler's Proof of Fermat's Little Theorem

Today: Euler's proof of FLT.

Recall that we defined the integers $C(n,k)$ by the equation

$$(a+b)^n = \sum_k C(n,k)\, a^k b^{n-k}$$

and then we used this equation to prove "Pascal's Recurrence"

$$C(n,k) = C(n-1,k-1) + C(n-1,k).$$

In order to finish Euler's proof we need to show that for all primes p we have

$$[C(p,k)]_p = [0]_p \text{ when } k \in \{1,2,\cdots,p-1\}.$$

The proof is based on the following theorem.

✡ Theorem: For all $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$,

$$C(n,k) = \frac{n!}{k!(n-k)!}.$$

Proof: Note that for all $n \geq 0$ we have

$$C(n,0) = C(n,n) = 1$$

and

$$\frac{n!}{0!\,n!} = \frac{n!}{n!\,0!} = 1,$$

so the result is true in these cases. Now let $n \geq 0$ and consider the following statement $P(n) :=$

"$C(n,k) = \frac{n!}{k!(n-k)!}$ for all $1 \leq k \leq n-1$".

We will prove by induction that $P(n)$ is true for all $n \geq 0$.

Base Case: We have already seen that $P(0)$ & $P(1)$ are true. That's good enough. ///

Induction Step: Now fix some $m \geq 1$ and assume for induction that $P(m-1)$ is true. In this case we want to show that $P(m)$ is also true. So consider any $1 \leq k \leq m-1$. Then we have

$$C(m,k) = C(m-1,k-1) + C(m-1,k) \qquad \text{(Pascal)}$$

$$= \frac{(m-1)!}{(k-1)!(m-k)!} + \frac{(m-1)!}{k!(m-k-1)!} \qquad \text{(P(m-1))}$$

$$= \frac{k}{k}\frac{(m-1)!}{(k-1)!(m-k)!} + \frac{(m-1)!}{k!(m-k-1)!}\frac{(m-k)}{(m-k)}$$

$$= \frac{k(m-1)!}{k!(m-k)!} + \frac{(m-1)!(m-k)}{k!(m-k)!}$$

$$= \frac{[k+(m-k)](m-1)!}{k!(m-k)!}$$

$$= \frac{m\cdot(m-1)!}{k!(m-k)!} = \frac{m!}{k!(m-k)!}$$ ✓

We conclude that $P(m)$ is true. ///

Therefore, by the Principle of Induction we conclude that $P(n)$ is true for all integers $n \geq 0$. ///

[Remark: That proof is perfectly valid, but is still doesn't explain where the formula $n!/(k!(n-k)!)$ comes from.

The usual way to derive this formula is to show that $C(n,k)$ equals the number of ways to choose k objects from a set of n objects.

(C is for "coefficient" and "choose" :o)

Then the formula follows from a counting argument. Unfortunately we don't have time to talk about that. I'll just mention that there is an alternative notation

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

"n choose k"]

Finally we can finish Euler's proof.

★ Theorem: Let p be prime. Then for all $1 \leq k \leq p-1$ we have

$$[C(p,k)]_p = [0]_p .$$

Proof: We are trying to show that

$$p \mid C(p,k) .$$

So consider the formula

$$C(p,k) = \frac{p!}{k!(p-k)!} .$$

This looks like a fraction but we know that it's really an integer. This means that the denominator must be canceled by factors in the numerator.

Note that p divides the numerator $p!$.

But I claim that p does <u>not</u> divide the denominator $k!(p-k)!$.

Indeed, suppose we had

$$p \mid k(k-1)\cdots 3\cdot 2\cdot 1\cdot (p-k)(p-k-1)\cdots 3\cdot 2\cdot 1.$$

Then by Euclid's Lemma p must divide one of the factors on the right. But since $1 \le k \le p-1$, all of these factors are strictly less than p. Contradiction.

We conclude that p divides the numerator but not the denominator. Hence

$$p \mid \frac{p!}{k!(p-k)!}. \qquad ///$$

This completes the proof of FLT. For reference let me state it again.

☆ Fermat's little Theorem:

Let $a, p \in \mathbb{Z}$ with p prime. Then we have

$$[a^p]_p = [a]_p. \qquad ///$$

For the purposes of HW6 it is useful to note the following consequence.

If $\gcd(a,p)=1$ (i.e. if $p \nmid a$) then we can cancel $[a]_p$ from both sides to get

$$[a^p]_p = [a]_p$$

$$[a]_p [a^{p-1}]_p = [a]_p [1]_p$$

$$[a^{p-1}]_p = [1]_p.$$

The RSA cryptosystem (which we'll discuss after the break) is based on a slight generalization of this: For all primes $p \neq q$ and $a \in \mathbb{Z}$ with $p \nmid a$ & $q \nmid a$ we have

$$[a^{(p-1)(q-1)}]_{pq} = [1]_{pq}.$$

You will prove this on HW 6.

//

Finally, you might wonder about

$$[C(n,k)]_m$$

for general integers k, m, n. This is actually a pretty cool story. To see a hint of it, let's reduce Pascal's Triangle mod 2.

The usual triangle is

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1

Now let's reduce the triangle mod 2:

1
1 1
1 0 1
1 1 1 1
1 0 0 0 1
1 1 0 0 1 1
1 0 1 0 1 0 1
1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 1
1 1 0 0 0 0 0 0 1 1
1 0 1 0 0 0 0 0 1 0 1
1 1 1 1 0 0 0 0 1 1 1 1

You can kind of see a pattern here. This is a "fractal" structure called

"Sierpinski's Triangle"

RSA Cryptosystem

The RSA Cryptosystem.

Problem: To send secret messages over an insecure channel, without the need for any previous private agreement.

Until the 1970s this problem (called "public key cryptography") was thought to be impossible. Also, until this time number theory was thought to have no practical application.

Following work of Diffie & Hellman (1976), Rivest-Shamir-Adleman (1983) set up the first practical "public key" cryptosystem, based on Fermat's little Theorem and the problem of prime factorization.

Despite extensive research since then, the "RSA cryptosystem" is still the most popular method of securing online communication.

Here's how it works.

Alice wants to receive secret messages from anyone in the world.

Step 1: Alice chooses two large primes $p \neq q$ and computes the product $n = pq$.

She choose some random integer e such that

- $1 < e < (p-1)(q-1)$
- $\gcd(e, (p-1)(q-1)) = 1$.

She uses the Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that

$$ex + (p-1)(q-1)y = 1.$$

Note that $[e]_{(p-1)(q-1)}[x]_{(p-1)(q-1)} = [1]_{(p-1)(q-1)}$.

Let $[d]_{(p-1)(q-1)} = [x]_{(p-1)(q-1)}$ be the standard form with

$$1 < d < (p-1)(q-1).$$

Finally, Alice publishes

$$(e, n),$$

called her public encryption key. She keeps secret

$$(d, n),$$

called her private decryption key. ///

Step 2: To send Alice a secret message, Bob first obtains her public key (e, n).

Then he converts his message to a number [or sequence of numbers] $m \in \mathbb{Z}$ such that $0 \leq m < n$. There are many standard ways to do this.

Then he computes the standard form of $m^e \bmod n$:

$$[c]_n = [m^e]_n$$

where $0 \leq c < n$. [we call e the "encryption exponent".]

Finally, he sends the number c to Alice.

///

Step 3: Alice decrypts the message as follows.

Using her private key (d, n) she computes

$$[r]_n = [c^d]_n$$

where $0 \leq r < n$. [we call d the "decryption exponent".]

Now I claim that $r = m$ is Bob's secret message.

↓

Proof: Recall that we have

$$ed = 1 + k(p-1)(q-1) \text{ for some } k \in \mathbb{Z}.$$

Then (working mod $n = pq$) we have

$$\begin{aligned} r &= c^d \\ &= (m^e)^d \\ &= m^{(ed)} \\ &= m^{(1+k(p-1)(q-1))} \\ &= m\,(m^{(p-1)(q-1)})^k \quad \text{mod } n. \end{aligned}$$

Assuming that $p \nmid m$ and $q \nmid m$, then by HW6.3 (generalization of FLT) we have

$$m^{(p-1)(q-1)} = 1 \quad \text{mod } n,$$

and hence

$$\begin{aligned} r &= m\,(m^{(p-1)(q-1)})^k \\ &= m\,(1)^k \\ &= m \quad \text{mod } n, \end{aligned}$$

as desired. ///

In the very unlikely case that $p|m$ or $q|m$ the result is still true but we don't have the technology to prove it. [The proof is based on the "Chinese Remainder Theorem".] ///

OK, great. But why is this system secure?

Suppose that Eve the eavesdropper is listening to all communications between Alice and Bob.

Then Eve knows the numbers

$$e, n, c$$

But she wants to know m. By the above calculation it is enough for Eve to know the decryption exponent d. And to find d she only needs to know the number $(p-1)(q-1)$; then she can compute

$$d \equiv e^{-1} \bmod (p-1)(q-1).$$

So here's the issue:

Eve knows $p \cdot q$ and she wants to know $(p-1)(q-1)$. Certainly she will able to compute this if she knows the prime factors p & q. So the security of the RSA cryptosystem comes down to the following assumption.

✡ Assumption:

It is computationally much more expensive for Eve to factor $n = p \cdot q$ into p & q than it is for Alice & Bob to perform the computations of encryption and decryption.

Years of experience suggest that this assumption is valid, but no one has proved a theorem to this effect. However, the system will break if quantum computers ever become practical.