

11/13/15

HW5 due Wed Nov 18

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

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

$$"n^p = n \pmod{p}"$$

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

$$"n^p = n \pmod{p}"$$

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

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

$$"1^p = 1 \pmod{p}" \quad \checkmark$$

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

$$"k^p = k \pmod{p}"$$

is a true statement.



In this case we will prove that

$$“(k+1)^p = (k+1) \pmod p”$$

is also a true statement. Indeed, we have

$$\begin{aligned} (k+1)^p &= k^p + 1^p \pmod p && (?) \\ &= k + 1 \pmod p && \text{base case} \\ &&& \text{\& assumption.} \end{aligned}$$

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

$$\begin{aligned} [(k+1)^p]_p &= [k^p + 1^p]_p && (?) \\ &= [k^p]_p + [1^p]_p \\ &= [k]_p + [1]_p \\ &= [k+1]_p \end{aligned}$$

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

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

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



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

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

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

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

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

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

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

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

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

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

and we want to know why this is true.

11/16/15

HW5 due Wed.

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.

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

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

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

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

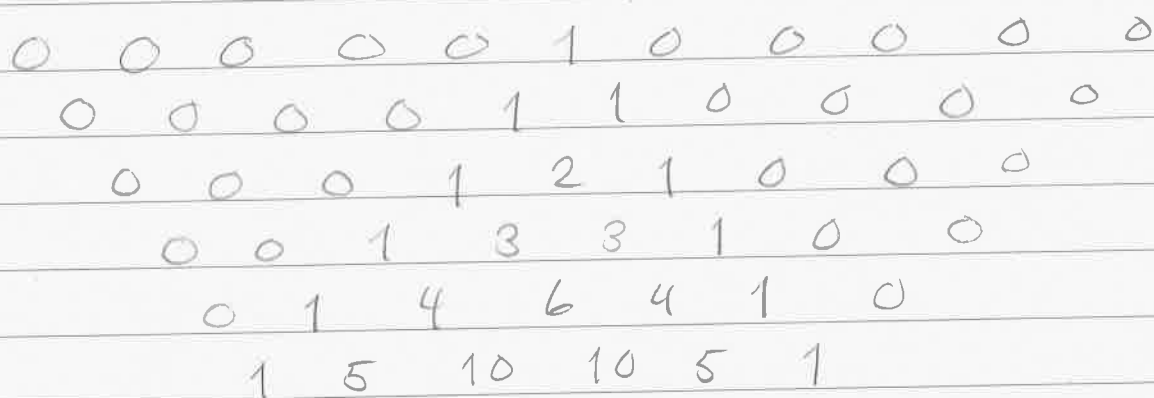
In general we see that

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



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":

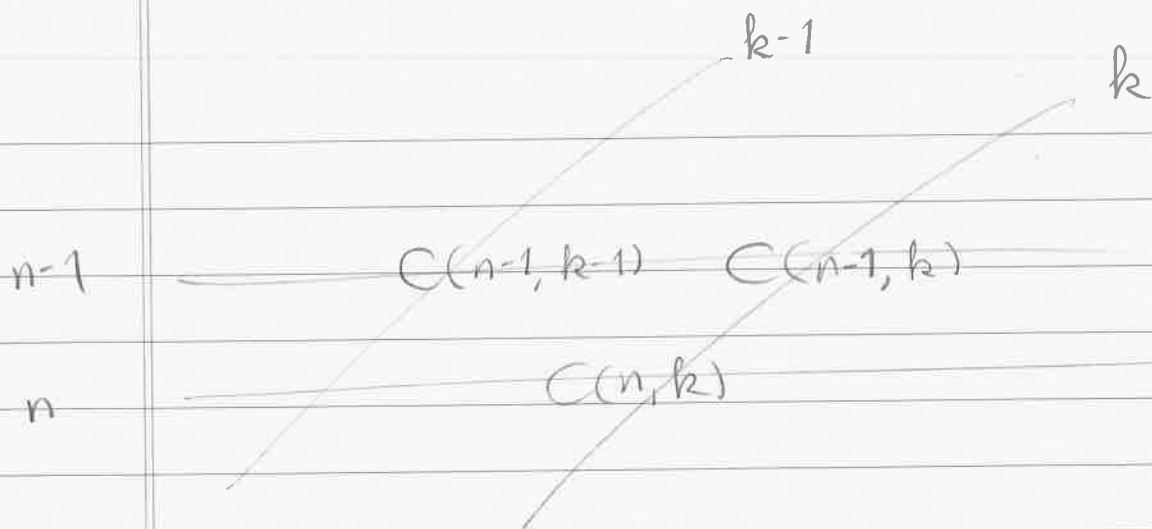


Here, each number is the sum of the two numbers above. Based on the picture above we predict that

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

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

If $C(n, k)$ is the entry in the n th row and the k th 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

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

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

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

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

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

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

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

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

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

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

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

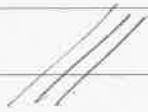
Then we replace $k+1$ by k in the first sum to get

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

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

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

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

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

$$= [n^p]_p + [1^p]_p + \underbrace{\sum_{k=1}^{p-1} [C(p, k)]_p [n^k]_p [1^{p-k}]_p}_{\text{We want to prove that this sum} = [0]_p .}$$

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

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

But the theorem we proved today does not immediately help with this. We really need a formula 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

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

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.



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

Example ($n=4$):

| | $C(4, k)$ | $\frac{4!}{(k!(4-k)!)}$ |
|-------|-----------|--|
| $k=0$ | 1 | $\frac{4!}{0!4!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{1 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 1 \checkmark$ |
| $k=1$ | 4 | $\frac{4!}{1!3!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{1 \cdot 3 \cdot 2 \cdot 1} = 4 \checkmark$ |
| $k=2$ | 6 | $\frac{4!}{2!2!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 2 \cdot 1} = 6 \checkmark$ |
| $k=3$ | 4 | $\frac{4!}{3!1!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 1} = 4 \checkmark$ |
| $k=4$ | 1 | $\frac{4!}{4!0!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 1} = 1 \checkmark$ |

It seems to work.

11/18/15

HW5 due now.

HW6 will be due Fri Dec 4.

Exam 3 is Mon Dec 7 in class.

Today: HW5 discussion.

On Friday we'll finish Euler's proof of Fermat's little Theorem.

After the Thanksgiving break we'll discuss the RSA cryptosystem and then review for Exam 3.

[Remark: We did a thorough discussion of Problem 2 from the homework. Please see the solutions online.]

11/20/15

I'll post HW6 today and it will be due on Fri Dec 4.

After the break we'll discuss the RSA cryptosystem and then we'll review for Exam 3 which is Mon Dec 7 in class.

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

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

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 $P(n) :=$

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

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

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

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

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

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

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

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

We conclude that $P(m)$ is true. \equiv

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

[Remark: That proof is perfectly valid, but it 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" 😊)

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 not 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 $1 \leq k \leq p-1$, all of these factors are strictly less than p . Contradiction.

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

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

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

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

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

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

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

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

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.

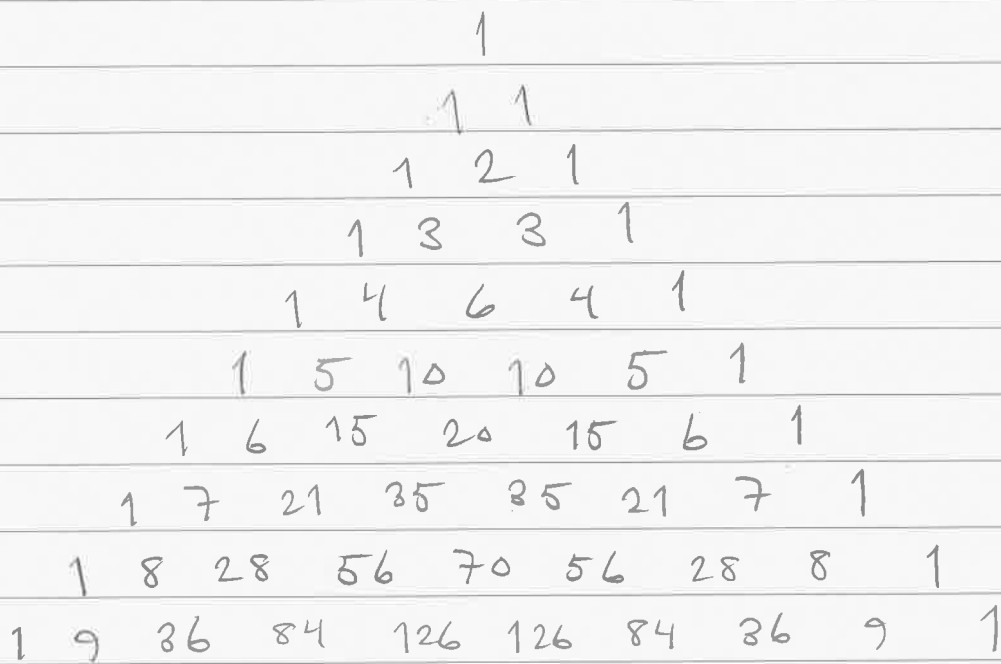


Finally, you might wonder about

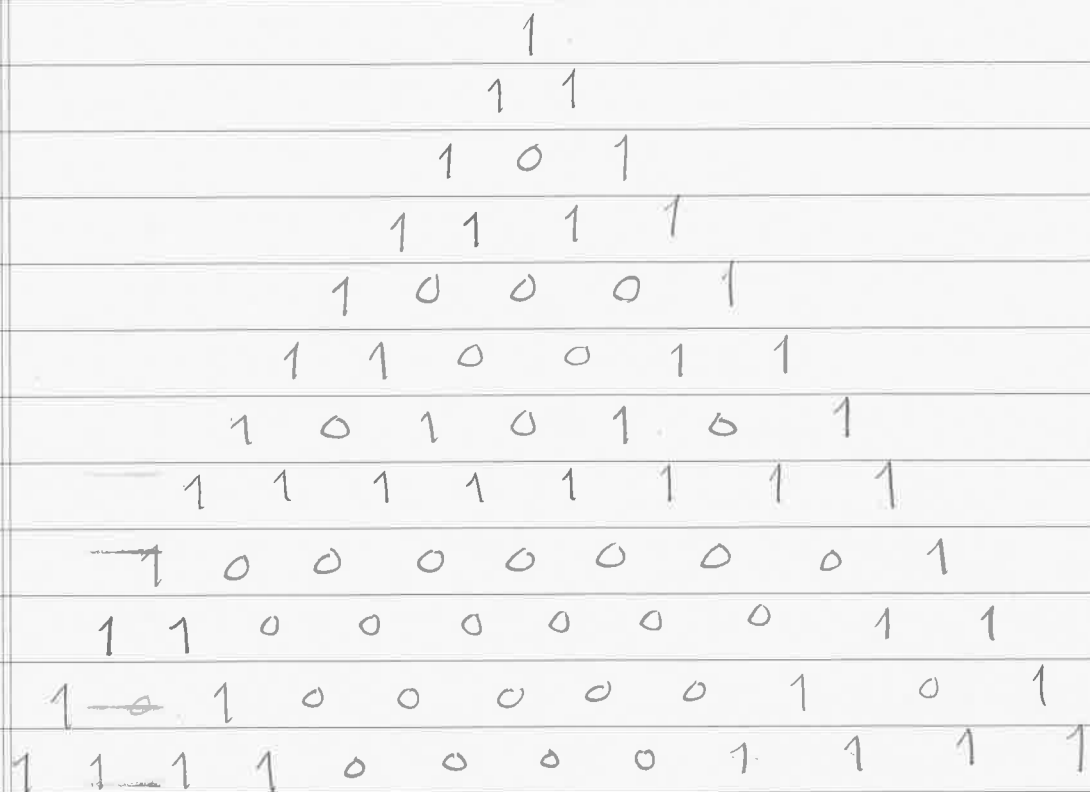
$$[C(n, k)]_m$$

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



Now let's reduce the triangle mod 2:



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

"Sierpinski's Triangle"

[see the handout.]

11/30/15

Final week of class.

Today & Wed: RSA Cryptosystem.

Fri: HW6 due, Review for Exam 3

Next Mon: Exam 3.

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 (1978) 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 chooses 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

$$\begin{aligned} r &= c^d \\ &= (m^e)^d \\ &= m^{(ed)} \\ &= m^{(1+k(p-1)(q-1))} \\ &= m \left(m^{(p-1)(q-1)} \right)^k \pmod{n}. \end{aligned}$$

Assuming that $p \nmid m$ and $q \nmid m$, then by HW6.2 (generalization of FLT) we have

$$m^{(p-1)(q-1)} = 1 \pmod{n},$$

and hence

$$\begin{aligned} r &= m \left(m^{(p-1)(q-1)} \right)^k \\ &= m (1)^k \\ &= m \pmod{n}, \end{aligned}$$

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

$$d = e^{-1} \pmod{(p-1)(q-1)}.$$

So here's the issue :

Eve knows $p \cdot q$ and she wants to know $(p-1)(q-1)$. Certainly she will be 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.

12/2/15

HW6 due Fri

Review session Fri

Exam 3 Mon.

I think we adequately covered the RSA cryptosystem last time, so today I'll give you some hints for HW6 and discuss the solutions to the practice exams.

HW6 Problem 1:

This problem has a secret agenda. We have seen the Binomial Theorem, which can be stated as follows:

For all integers $n \geq 0$ and all numbers x we have

$$(1+x)^n = \sum_{k=0}^n \frac{n!}{k!(n-k)!} x^k.$$

But we also know that $(1+x)^n$ sometimes makes sense when $n < 0$.

For example, you probably recall the following theorem on the "geometric series".

★ Geometric Series: If x is any number with $|x| < 1$ then we have a convergent power series expansion

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

Replacing x by $-x$ in this formula gives

$$(1+x)^{-1} = (1-(-x))^{-1}$$

$$= \frac{1}{1-(-x)}$$

$$= 1 + (-x) + (-x)^2 + (-x)^3 + \dots$$

$$= 1 - x + x^2 - x^3 + \dots$$

Is this related to the Binomial Theorem?

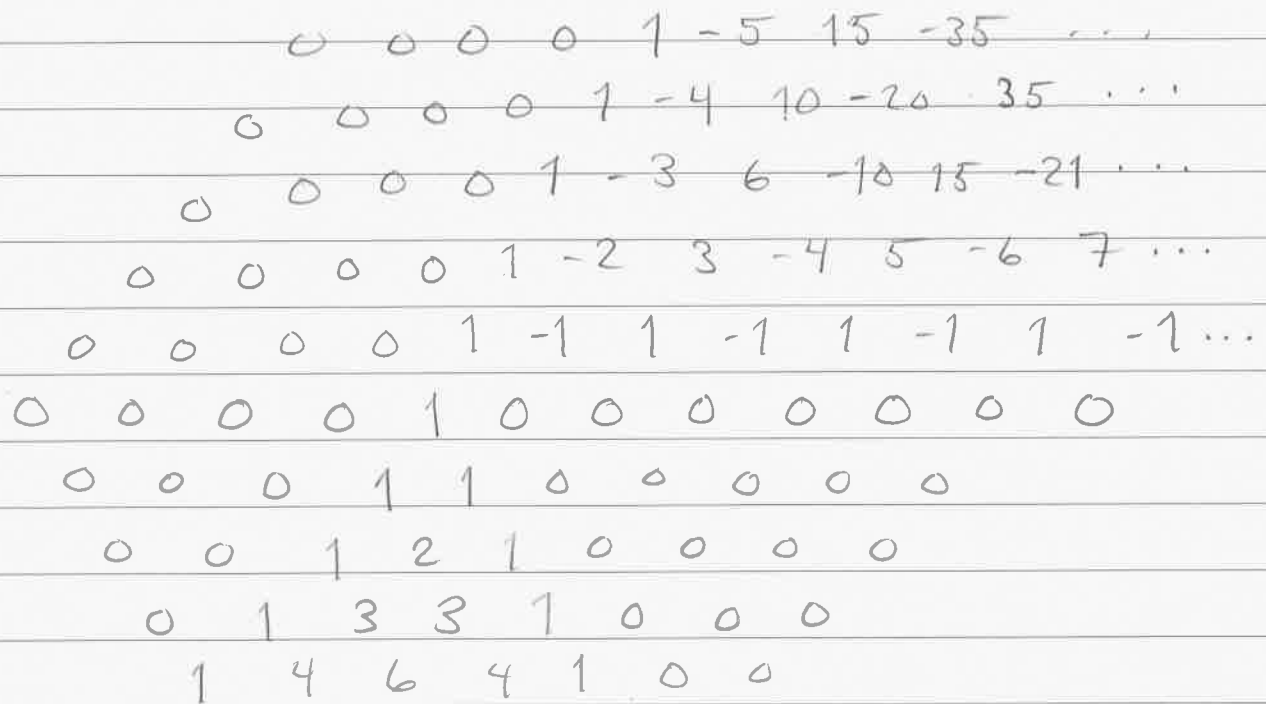
Is it related to Pascal's Triangle?

The idea is to try to extend Pascal's Triangle going upward. Let begin by assuming that

- $C(n, k) = 0$ when $k < 0$

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

Then by extending the usual Pascal Recurrence upwards we obtain



That's kind of strange. It looks like we obtain a rotated copy of Pascal's Triangle with some negative signs in it.

It also seems that this gives us the correct answer for expanding negative powers of $1+x$. For example, if we differentiate both sides of

$$(1+x)^{-1} = 1 - x + x^2 - x^3 + \dots$$

we obtain

$$-(1+x)^{-2} = 0 - 1 + 2x - 3x^2 + 4x^3 - \dots$$

$$(1+x)^{-2} = 1 - 2x + 3x^2 - 4x^3 + \dots$$

which agrees with the triangle. In general we will define the "binomial coefficients" $C(n, k)$ by the formula

$$(1+x)^n = \sum_k C(n, k) x^k$$

even when n or k is negative.

The goal on HW6 Problem 1 is to show that everything still makes sense. In particular you will show that for $n \geq 0$ we have

$$(1+x)^{-n} = \sum_{k=0}^{\infty} (-1)^k \frac{(n+k-1)!}{k!(n-1)!} x^k,$$

which is called Newton's generalized binomial theorem (1665). He discovered this while he was inventing Calculus.

There is another very cool interpretation for the numbers $C(n, k)$ when $n < 0$.

Recall that when $n \geq 0$ and $k \geq 0$ we sometimes write

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

"n choose k".

This is the number of ways to choose an unordered collection of k objects from a set of n objects. For example, consider the set of 3 objects

$$\{1, 2, 3\}.$$

The number of ways to choose two elements is

$$\binom{3}{2} = \frac{3!}{2!1!} = \frac{3 \cdot \cancel{2} \cdot 1}{\cancel{2} \cdot 1} = 3$$

Indeed, the choices are

$$\{1, 2\}, \{1, 3\}, \{2, 3\}$$

Now suppose we are allowed to repeat our choices. For example, suppose that

$$\{1, 1, 3, 3, 3\}$$

is a valid choice. Let's define the number

$$\binom{n}{k} := \text{number of ways to choose } k \text{ objects from } n \text{ objects with } \underline{\text{repetition allowed}}.$$

Then one can show that

$$\binom{n}{k} = \binom{n+k-1}{k}$$



Instead of proving this in the final 5 minutes of the course, let me just show you an example.

Example ($n=3, k=4$):

The formula says

$$\binom{3}{4} = \binom{3+4-1}{4} \\ = \binom{6}{4} = 15$$

The ways to choose 4 elements of the set $\{1, 2, 3\}$ are

1111, 1112, 1113

1122, 1123, 1133

1222, 1223, 1233, 1333

2222, 2223, 2233, 2333, 3333

Note that there are 15 choices. ✓

Finally, I'll end the course with a weird formula. According to HW 6.1 we have

$$\binom{-n}{k} = (-1)^k \binom{n}{k}$$

What could this possibly mean ?!

THE END.

12/4/15

HW6 due now.

Exam 3 on Monday.

Today: Review for Exam 3.

① Equivalence Relations

Let S be a set we say that " \sim " is an equivalence relation on S if

- $\forall x \in S, x \sim x$
- $\forall x, y \in S, x \sim y \Rightarrow y \sim x$
- $\forall x, y, z \in S, (x \sim y \wedge y \sim z) \Rightarrow x \sim z.$

Examples: The set

$$\mathbb{Q} := \{ [a, b] : a, b \in \mathbb{Z}, b \neq 0 \}$$

with $[a, b] \sim [c, d] \iff ad = bc.$

For $0 \neq n \in \mathbb{Z}$ the set

$$\mathbb{Z}/n := \{ [a]_n : a \in \mathbb{Z} \}$$

with $[a]_n \sim [b]_n \iff n \mid (a - b).$ //

Be able to prove that both of these are equivalences. Be able to prove that the following algebraic operations are well-defined.

$$[a, b] \cdot [c, d] = [ac, bd]$$

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a]_n \cdot [b]_n = [ab]_n$$

$$[a]_n + [b]_n = [a + b]_n$$

② Modular Arithmetic.

Explain why

$$\mathbb{Z}/n = \{ [0]_n, [1]_n, \dots, [n-1]_n \}$$

Hint: This is just the Division Theorem in disguise.

Explain why $[a]_n$ has a multiplicative inverse (i.e. $\exists x \in \mathbb{Z}, [a]_n \cdot [x]_n = [1]_n$) if and only if $\gcd(a, n) = 1$.

Hint: Bézout's Identity.

③ Induction.

The Principle of Induction says the following:

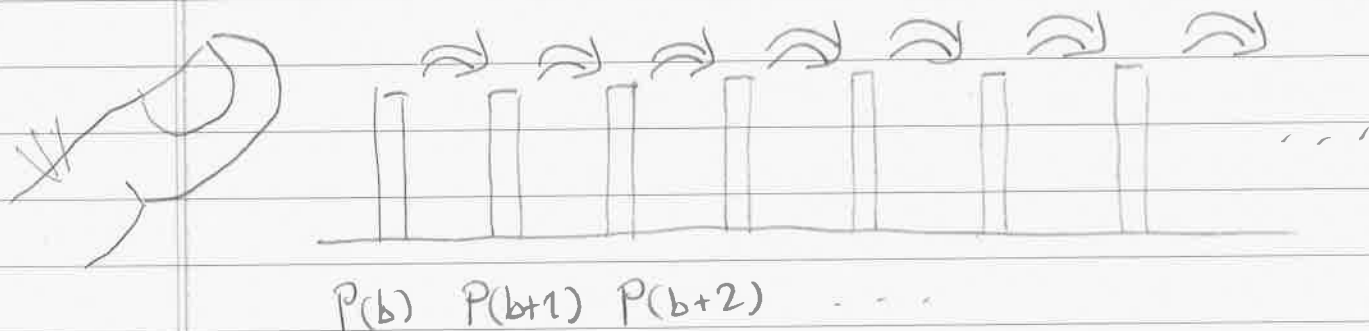
Let $P(n)$ be a logical statement depending on an integer n . IF

- $P(b) = T$ for some $b \in \mathbb{Z}$, and
- For all $k \geq b$ we have

$$P(k) \Rightarrow P(k+1) ,$$

then it follows that $P(n) = T \quad \forall n \geq b$.

[Analogy : Knocking down dominoes.



The base case is your finger, The induction step is gravity.

Example: Prove that $2 \mid (3^n - 1) \forall n \geq 1$.

Proof: Let $P(n) = "2 \mid (3^n - 1)"$.

• Base Case: $P(1) = "2 \mid 2" = T \checkmark$

• Induction Step: Fix $k \geq 1$ and assume for induction that $P(k) = T$, i.e., assume $\exists l \in \mathbb{Z}$ with $3^k - 1 = 2l$.

In this case we will show that $P(k+1) = T$. Indeed, we have

$$\begin{aligned} 3^{k+1} &= 3 \cdot 3^k \\ &= 3(2l + 1) \\ &= 6l + 3 \\ &= 2(3l + 1) + 1 \end{aligned}$$

$$\implies 3^{k+1} - 1 = 2(3l + 1). \quad \checkmark$$

By the POI we have $P(n) = T \forall n \geq 1$.

When the technique of induction is combined with more complicated mathematics you need to keep the logic and the math separate in your mind.

④ Binomial Theorem.

It says the following: let a, b be any numbers and let $n \in \mathbb{Z}$ with $n \geq 0$. Then

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

How did we prove this? We defined

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

Then we proved

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

Then we used induction on n to prove

$$" C(n, k) = \frac{n!}{k!(n-k)!} \text{ for } 0 \leq k \leq n "$$

is true for all $n \geq 1$. [The details are on both practice exams.]



⑤ Fermat's little Theorem.

It says: For all $b, p \in \mathbb{Z}$ with p prime we have

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

If, moreover, $p \nmid b$ then we can cancel $[b]_p$ from both sides to get

$$[b^{p-1}]_p = [1]_p. \quad \equiv$$

How did we prove it?

Proof: Induction on b . Fix a prime p and let $P(b) = "[b^p]_p = [b]_p"$.

- Base Case: $P(0) = "[0^p]_p = [0]_p" = T \quad \checkmark$
- Fix $k \geq 0$ and assume $[k^p]_p = [k]_p$.
Then we have

$$\begin{aligned} [(k+1)^p]_p &= [k^p]_p + [1^p]_p && \text{(why?)} \\ &= [k]_p + [1]_p && \text{(by } P(k)) \\ &= [k+1]_p. \end{aligned}$$

\equiv

(6) Freshman's Dream

It says: Let $a, b, p \in \mathbb{Z}$ with p prime. Then

$$(*) \quad [(a+b)^p]_p = [a^p]_p + [b^p]_p.$$

We proved this by showing that

$$p \mid \frac{p!}{k!(p-k)!} \quad \text{when } k \in \{1, 2, \dots, p-1\}.$$

Explain why this implies (*).

Hint: Binomial Theorem.

THE END.