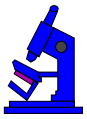
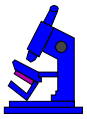



Chapter 3

Lecture 3 - Preliminaries


Administrivia

- Unfortunately, we have been unable to purchase a SIM card reader. If you know where to get one, please contact Hugh...
- We hope to start Lab1 next week, but the room is still not ready. I will email you when I know...
- Successful project bids announced on Monday, pick up equipment at that time.



Motivation: fields

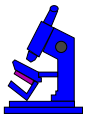
Finite fields are found over and over again particularly in cryptography and error detection. Found in:

- ✔ Diffie-Hellman relies on apparent difficulty of computing logarithms over $GF(q)$
- ✔ ElGamal cryptosystems, elliptic curves
- ✔ Zero-knowledge proof protocols
- ✔ AES encryption (in GF)

Consider: Stupid system: Z_{15}

*	0	1	2	3	4	5	6	7	8	9	10	11	...
0	0	0	0	0	0	0	0	0	0	0	0	0	...
1	0	1	2	3	4	5	6	7	8	9	10	11	...
2	0	2	4	6	8	10	12	14	1	3	5	7	...
3	0	3	6	9	12	0	3	6	9	12	0	3	...
4	0	4	8	12	1	5	9	13	2	6	10	14	...
5	0	5	10	0	5	10	0	5	10	0	5	10	...
6	0	6	12	3	9	0	6	12	3	9	0	6	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...

1,2,4 have unique inverse, but the others not.

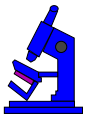


Consider: Stupid system: Z_{15}

If our rule was: multiply code symbol by key symbols 4,2,1 decode by dividing (i.e. multiplying by inverse)

- ✔ Then 3,5,9 encodes to $4 * 3, 2 * 5, 1 * 9 = 12, 10, 9$. We decode with $12 * 4, 10 * 8, 9 * 1 = 3, 5, 9$
- ✘ However, choosing other keys without unique inverses will cause problems.

Back to operations in $GF(p^n)$...



Why primes?

In the book “Contact”, the heroine recognizes an alien communication because it starts...

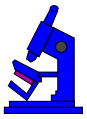
2.. 3.. 5.. 7.. 11.. 13.. 17.. 19.. 23...[2]

[2] Actually 1,2,3,5... :)

Why primes?

Is it just a coincidence that the numbers on the main Real Madrid player’s jerseys are:

Carlos, No 3; Zidane, No 5; Raul, No 7; Owen, No 11?



Why primes?

For 2500 years mathematicians studied prime numbers just because they were interesting, without any idea they would have practical applications. Possible real-world uses:

1. Sometimes... a prime number of ball bearings arranged in a bearing, to cut down on periodic wear (also *gear* teeth).

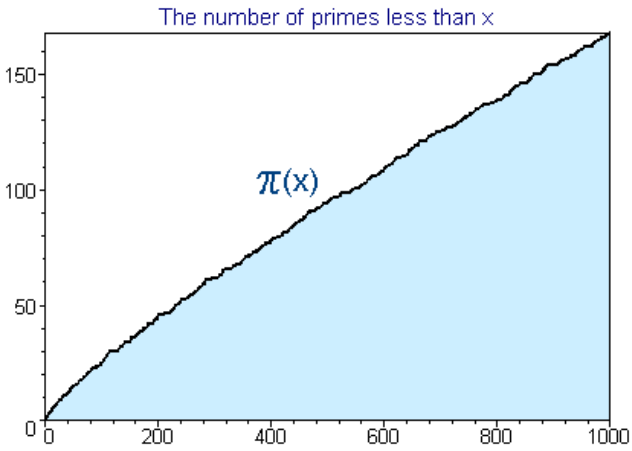
2. Possibly... the 13 and 17-year periodic emergence of cicadas may be due to coevolution with predators (that lost and became extinct).

Why primes?

✔ We do not know how to guess when the next one will occur

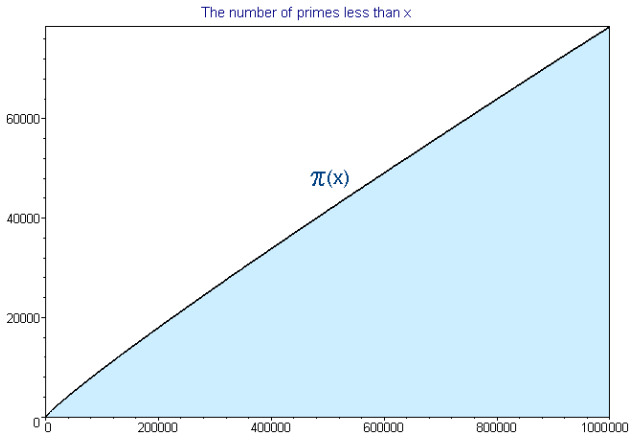
✔ But ... we do know that the density is predictable...

Why primes?

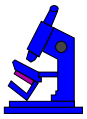


(113-127)

Why primes?



(Asymptotic to $\frac{x}{\log x}$)



Why primes?

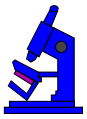
- ✔ Because 2500 years of mathematics has failed to uncover some basic prime properties, they make a good candidate for constructing difficult (impossible to decrypt) translations... and hence our interest in them...
- ✔ Because primes are beautiful...

Why primes?

Consider the following problem:

Is it possible to find an arbitrary sized sequence of numbers that are not primes?

Answer: **YES!**



Not primes...

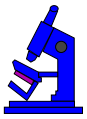
If you want 3 not-primes in a row, calculate $4 * 3 * 2 * 1 = 4!$, and choose the numbers $4! + 2$, $4! + 3$ and $4! + 4$. None can be a prime.

If you want 42,000 not-primes in a row, calculate $42001 * \ldots * 2 * 1 = 42001!$, and choose the numbers $42001! + 2$, $42001! + 3$... None can be a prime.

If you want 484758476584377537598348750948594549584 0 not-primes ...

Fermat's little theorem

- ✔ In cryptography, one often wants to raise a number to a power, modulo another number.
- ✔ For the integers mod p where p is a prime (denoted Z_p), there is a result know as Fermat's little theorem, discovered by the 17th century French mathematician Pierre de Fermat, 1601-1665.



Fermat's little theorem

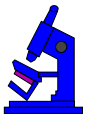
Theorem (Fermat): If p is a prime and a is any non-zero number less than p, then

$$a^{p-1} \bmod p = 1$$

Notation: sometimes use $a^{p-1} \bmod p = 1$, and sometimes $a^{p-1} \equiv 1 \pmod{p}$. Exponentiation in a field.

Fermat's little theorem, $p = 11$

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1



Fermat's little theorem

- ✔ For $p = 11$ the value is always 1 by the time the power gets to 10
- ✔ Sometimes the value gets to 1 earlier
- ✔ Lengths of runs are always numbers that divide evenly into 10
- ✔ A value of a for which the whole row is needed is called a *generator*. 6, 7, and 8 are generators.

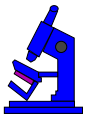
An interesting observation..

Because a to a power mod p always starts repeating after the power reaches $p - 1$, you can do this:

$$a^x \bmod p = a^{x \bmod (p-1)} \bmod p.$$

Thus modulo p in the expression requires modulo $p - 1$ in the exponent. For $p = 13$, then

$$a^{29} \bmod 13 = a^{29 \bmod 12} \bmod 13 = a^5 \bmod 13.$$



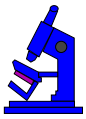
Another example

$$\text{result} \quad = \quad 7^{1215} \bmod 13$$

Another example

result=

622470275067322737046556455907979268906239864832921913090207877109248699107274058706519890781017383899497826793481300967770892782660131355777365361484044783800851222817392261341421370762400507026834564501614788818580162335818155077291900607338638109858209984177537766703728681473967012031571239691400018482234035235590645515566753410247396453541377412583676260706359331048403293779053704648771069764131865422622995052805575842805741858026942132998022801793254945606289489407393444822846491511971411686989595879473202428574269018023244940256710105083114967356334295809219455711191131246974627173111242792554453321165049145300772419961893572985086052067801207898808355252223419405145855673208684204238889320915704079986487190106499123086028865754587854838031902109935110264503891544145872580747830622294066978047059698088822497677940491279201763309541131855593877680081677862469580790949705787192596277127796303487781814106147375370904627195995589087276
8469943 mod 13 = 5



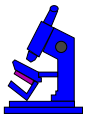
How did I work that out?

I used bc

An arbitrary precision calculator language

Another example

result $= 7^{1215} \bmod 13$

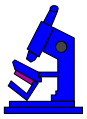


Another example

$$\begin{aligned} \text{result} &= 7^{1215} \bmod 13 \\ &= 7^{1215} \bmod 12 \bmod 13 \end{aligned}$$

Another example

$$\begin{aligned} \text{result} &= 7^{1215} \bmod 13 \\ &= 7^{1215} \bmod 12 \bmod 13 \\ &= 7^{3} \bmod 13 \end{aligned}$$

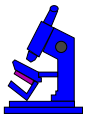


Another example

$$\begin{aligned} \text{result} &= 7^{1215} \bmod 13 \\ &= 7^{1215 \bmod 12} \bmod 13 \\ &= 7^3 \bmod 13 \\ &= 343 \bmod 13 \end{aligned}$$

Another example

$$\begin{aligned} \text{result} &= 7^{1215} \bmod 13 \\ &= 7^{1215 \bmod 12} \bmod 13 \\ &= 7^3 \bmod 13 \\ &= 343 \bmod 13 \\ &= 5 \end{aligned}$$

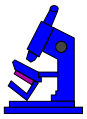


Summary

We can do BIG NUMBER maths without calculating BIG numbers.

Euler

The Swiss mathematician Leonhard Euler (1707-1783) discovered a generalization of Fermat's Theorem which will later be useful in the discussion of the RSA cryptosystem.



Euler's theorem

Theorem (Euler): If n is any positive integer and a is any positive integer less than n with no divisors in common with n, then

$$a^{\phi(n)} \bmod n = 1,$$

where $\phi(n)$ is the *Euler phi function*:

$$\phi(n) = n(1 - 1/p_1) \ldots (1 - 1/p_m),$$

and $p_1, \ldots, p_m$ are all the prime numbers that divide evenly into n, including n itself in case it is a prime.

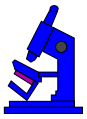
Special case 1

✔ If n is a prime, then using the formula,

$$\phi(n) = n(1 - 1/n) = n(\frac{n-1}{n}) = n - 1$$

Fermat's result is a special case of Euler's.

$$a^{\phi(n)} \bmod n = a^{n-1} \bmod n = 1$$



Special case 2

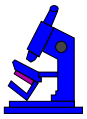
✔ Another special case needed for RSA comes when the modulus is a product of two primes: $n = pq$. Then

$$\phi(n) = n(1 - 1/p)(1 - 1/q) = (p - 1)(q - 1)$$

Special case 2

$$a^{(p-1)(q-1)} \bmod pq = 1$$

- assuming a has no divisors in common with pq
- and p and q are primes



Euler in action: $n = 15$ and $\phi(n) = 8$

a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}
4	8	1	2	4	8	1	2	4	8	1	2	4
9	12	6	3	9	12	6	3	9	12	6	3	9
1	4	1	4	1	4	1	4	1	4	1	4	1
10	5	10	5	10	5	10	5	10	5	10	5	10
6	6	6	6	6	6	6	6	6	6	6	6	6
4	13	1	7	4	13	1	7	4	13	1	7	4
4	2	1	8	4	2	1	8	4	2	1	8	4
6	9	6	9	6	9	6	9	6	9	6	9	6
10	10	10	10	10	10	10	10	10	10	10	10	10
1	11	1	11	1	11	1	11	1	11	1	11	1
9	3	6	12	9	3	6	12	9	3	6	12	9
4	7	1	13	4	7	1	13	4	7	1	13	4
1	14	1	14	1	14	1	14	1	14	1	14	1

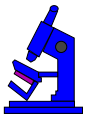
Table

Table illustrates Euler's theorem for $n = 15 = 3 \cdot 5$, with

$$\phi(15) = 15 \cdot (1 - 1/3) \cdot (1 - 1/5) = (3 - 1) \cdot (5 - 1) = 8$$

Notice here that a 1 is reached when the power is 8, but only for numbers with no divisors in common with 15.

For other base numbers, the value never gets to 1.



Euler

Arithmetic in the exponent is taken mod $\phi(n)$, so that, if a has no divisors in common with n,

$$a^x \bmod n = a^{x \bmod \phi(n)} \bmod n.$$

If $n = 15$ as above, then $\phi(n) = 8$, and if neither 3 nor 5 divides evenly into a, then $\phi(n) = 8$. Thus for example,

$$a^{28} \bmod 15 = a^{28 \bmod 8} \bmod 15 = a^4 \bmod 15.$$

Before we leave Euler...

We are interested in...

- ✔ Large prime numbers (p, q)
- ✔ Their product $n = pq$
- ✔ The Euler phi function $\phi(n) = (p-1)(q-1)$