Math 312, lecture 4, 18/5/2018

Last time: (1) Bezout's thm
(2) Linear equations — Bezout's thm gives one solution; unique factorization gives others

divisors of p are ±1, ±p → (3) Primes: 0, 1
- every integer is a pdt of primes
- Infinitely many primes

p|ab ⇒ p|a or p|b → (4) Primes: - the product is unique

Today: Examples

Factoring by trial division

Start with integer, e.g. 224

- try to divide by 2: $224 = 2 \cdot 112$
- try 2 again: $112 = 2 \cdot 56$
- try 2 again: $56 = 2 \cdot 28$
  $28 = 2 \cdot 14$
  $14 = 2 \cdot 7$
- $2 \nmid 7$ so 7 is prime: $3 > \sqrt{7}$ so no need to check further

Observe: smallest non-trivial divisor of $n \geq 2$ is prime. if p smallest divisor, $a|p$ then $a|n$ so can't have $1 < a < p$.

Infinitude of primes

Last time: pf by contradiction

(If set of primes is finite, find prime not in the set).

Algorithmic pf:

Algorithm: (0) $P = \{2\}$

(1) Let $n = \prod_{p \in P} p$ (pdt of all primes so far)

(2) Factor $n+1$ into primes

(3) Add all primes from step (2) into P

(4) return to step (1)

Key (last time): all primes from step 3 are "new" - not in P already

- Every time around the set P increases

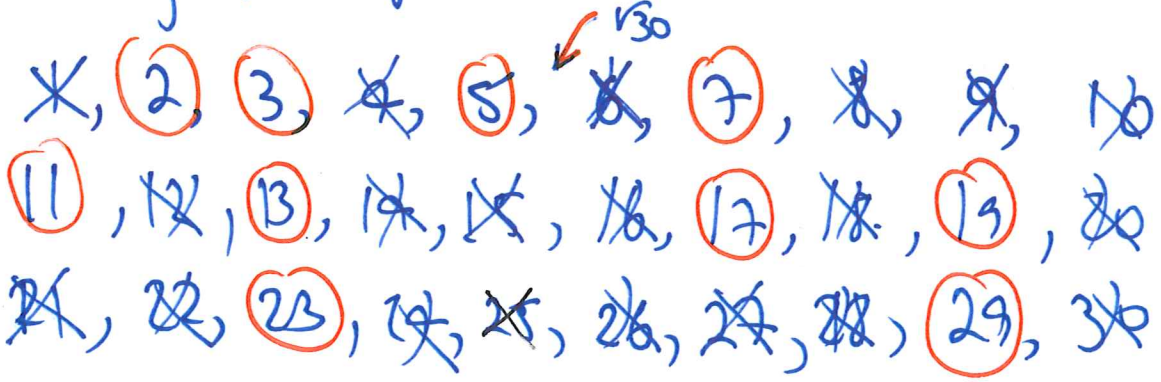
- Start with $P = \{2\}$, $n = 2$, $n+1 = 3$ prime
- $P = \{2, 3\}$, $n = 6$, $n+1 = 7$, prime
- $P = \{2, 3, 7\}$, $n = 42$, $n+1 = 43$, prime
- $P = \{2, 3, 7, 43\}$, $n = 1806$, $n+1 = 1807 = 13 \cdot 139$
- $P = \{2, 3, 7, 13, 43, 139\}$

$43 = 2 \cdot 3 \cdot 7 + 1$, so $2, 3, 7 \nmid 43$, $43 = 5 \cdot 8 + 3$ so $5 \nmid 43$

$\sqrt{43} \leq \sqrt{49} = 7$

Finding all primes

Want primes up to 30



(0) Listed integers up to n, strike 1 (not prime)

(1) smallest number left is prime

(2) strike all multiples of prime just found

(3) return to step (1)

Method is called "sieve of Erathosthenes".

Hard to use sieves to count primes, can count numbers of form pq.

Thm: (Chen) $\exists \infty$'ly many primes p s.t. $p+2$ is a pdt of two primes

Thm: (Zhang 2013) $\exists \infty$'ly pairs $p, p+k$ both prime, $k \leq 7 \cdot 10^{7}$

Primes of special form

- twin primes ($p, p+2$ both prime)
- Mersenne primes: $p = 2^k - 1$. (eg. $3 = 2^2-1$, $7 = 2^3-1$, $31 = 2^5-1$ ...)

Ex: if $a^k - b^k$ is prime then k is prime, $a-b=1$, $a=2$, $b=1$

6 is perfect: $1+2+3 = 6 = 3 \cdot 2$

28 is perfect: $1+2+4+7+14 = 28 = 7 \cdot 4$

Thm: If n is even, n is perfect iff $n = 2^{k-1}(2^k-1)$ where 2^k-1 is prime

Question: (1) Are there ∞'ly many Mersenne primes/even perfect numbers?

(2) Are there odd perfect numbers?

- Fermat numbers: $F_n = 2^{2^n}+1$

$F_0 = 2^1+1 = 3$, $F_1 = 2^2+1 = 5$, $F_2 = 2^4+1 = 17$

$F_3 = 2^8+1 = 257$, $F_4 = 2^{16}+1 = 65,537$ ← prime

Fermat Conj: F_n all prime

Euler: $641 \mid F_5 = 2^{32}+1 \approx 4 \cdot 10^9$

No further prime Fermat numbers known.

Asides Cole, October 1903 meeting of the AMS:

$$2^{67}-1 = 193,707,721 \times 761,838,257,287$$

Application of Euclid's method to Fermat numbers

Calc: Say $x \in \mathbb{Z}$ what is $(x^2+1, x+1)$?

By Euclid, $(x^2+1, x+1) = (x+1, x^2-x)$ ← $(x^2+1)-(x+1)$

$= (x+1, x(x-1))$

$= (x+1, x-1) = (x+1, 2) = \begin{cases} 1 & x \text{ even} \\ 2 & x \text{ odd} \end{cases}$

$(x+1, x) = 1$ so can remove x

$2 = (x+1)-(x-1)$

Cor: Note $F_{n+1} = 2^{2^{n+1}}+1 = 2^{2^n \cdot 2}+1 = (2^{2^n})^2+1$

$F_n =$ $\qquad = 2^{2^n}+1$

so $(F_{n+1}, F_n) = 1$

What about (F_n, F_m)?

try

$$(F_{m+2}, F_m) = (2^{2^m \cdot 4} + 1, 2^{2^m} + 1)$$

subtraction ↘

$$= (2^{2^m \cdot 4} - 2^{2^m}, 2^{2^m} + 1)$$

subtract

$$= (2^{2^m}(2^{2^m \cdot 4 - 2^m} - 1), 2^{2^m} + 1)$$

2^{2^m} prime to $2^{2^m}+1$ ↘

$$= (2^{2^m \cdot 3} - 1, 2^{2^m} + 1)$$

addition ↘

$$= (2^{2^m \cdot 3} + 2^{2^m}, 2^{2^m} + 1)$$

common factor ↘

$$= (2^{2^m}(2^{2^m \cdot 2} + 1), 2^{2^m} + 1)$$

2^{2^m} is "irrelevant" (prime to $2^{2^m}+1$) ↘

$$= (2^{2^{m+1}} + 1, 2^{2^m} + 1)$$

$$= (F_{m+1}, F_m) = 1$$

Thm: $(F_m, F_n) = 1$ if $m \neq n$

Cor: Infinitely many primes

Pf of Thm: Say $n = m + k$ so $F_n = 2^{2^{m+k}} + 1 = 2^{2^m \cdot 2^k} + 1$

Show: $(2^{2^m \cdot a} + 1, 2^{2^m} + 1) = (2^{2^m \cdot (a-2)} + 1, 2^{2^m} + 1)$

Indeed,

$$(2^{2^m \cdot a}+1,\ 2^{2^m}+1) = (2^{2^m \cdot a}-2^{2^m},\ 2^{2^m}+1)$$

$$= (2^{2^m}(2^{2^m(a-1)}-1),\ 2^{2^m}+1)$$

$$= (2^{2^m(a-1)}-1,\ 2^{2^m}+1)$$

$$= (2^{2^m(a-1)}+2^{2^m},\ 2^{2^m}+1)$$

$$= (2^{2^m}(2^{2^m(a-2)}+1),\ 2^{2^m}+1) = (2^{2^m(a-2)}+1,\ 2^{2^m}+1).$$

Set $d(a) = (2^{2^m \cdot a}+1,\ 2^{2^m}+1)$

Then $(F_{m+k}, F_m) = d(2^k) = d(2^k-2) = d(2^k-4) = d(2^k-6)$

$= \cdots = d(2) = (2^{2^m \cdot 2}+1,\ 2^{2^m}+1) = (F_{m+1}, F_m) = 1.$

↑ count down even numbers

If $(a,c)=1$ then $(a,bc)=(a,b)$ ← PS2

here $a = 2^{2^m}+1$, $b = 2^{2^m(a-1)}-1$, $c = 2^{2^m}$.

Using Unique factorization

Notation: $24 = 2^3 \cdot 3 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdots$

$15 = \quad = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdots$

Write: $n = \prod_p p^{e_p}$ where $e_p \in \mathbb{Z}_{\geq 0}$ all but finitely many are 0

Say $m = \prod_p p^{f_p}$. What is $nm = \prod_p p^{e_p + f_p}$

Conversely, if $f_p \leq e_p$ for all p, $\frac{n}{m} = \prod_p p^{e_p - f_p}$

Shows: $m \mid n$ iff $f_p \leq e_p$ for all p

Similarly, say $d = \prod_p p^{g_p}$ divides both m, n.

Then $g_p \leq e_p$, $g_p \leq f_p$ so $g_p \leq \min\{f_p, e_p\}$

(if $d \mid 24$ and $d \mid 15$ then $d = 2^0 \cdot 3^{\{0 \text{ or } 1\}} \cdot 5^0 \cdot 7^0 \cdots$)

$\Rightarrow \gcd(m,n) = \prod_p p^{\min\{e_p, f_p\}}$

Similarly: $\operatorname{lcm}(m,n) = \prod_p p^{\max\{e_p, f_p\}}$

So: $\gcd(m,n) \cdot \operatorname{lcm}(m,n) = \prod_p p^{\min\{e_p, f_p\} + \max\{e_p, f_p\}}$

$= \prod_p p^{e_p + f_p} = mn$

Conclusions $\operatorname{lcm}(a,b) = \dfrac{a \cdot b}{\gcd(a,b)}$