Lecture 10

Test based on HW 1-3, Ch 1-13.

6 questions, 4 from HW, 2 from suggested.

Primes 3 mod 4 Thm:

There are ∞ many primes $\equiv 3 \bmod 4$.

Start with $\{7\}$

$A = 4\times7+3 = 31$

$\{7, 31\}$

$A = 4\times7\times31+3 = 871 = 13\times67$, $67 \equiv 3 \bmod 4$

$\{7, 31, 67\}$

$A = 4\times7\times31\times67+3 = 58159 = 19\times3061$, $19 \equiv 3 \bmod 4$

. . .

This method does not work for primes $\equiv 1 \bmod 4$.

Start with $\{p_1, \cdots, p_r\}$, $p_r \equiv 1 \bmod 4$, and form $A = 4p_1\cdots p_r + 1$ and factor $= q_1 \cdots q_s$

In this case, we may not have that one of $q_i \equiv 1 \bmod 4$

$\{5\}$

$A = 4\times5+1 = 21 = 3\times7$

i.e. $A \equiv 1 \bmod 4$ does not imply $q_j \equiv 1 \bmod 4$ for some j.

In general, m positive integer. we can separate primes into $\phi(m)$ families. (need to exclude $p|m$)

$\gcd(a,m)=1$, $S_a = \{p : p \equiv a \bmod m\}$

Dirichlet's thm on arithmetic progressions: Primes are evenly distributed among $\phi(m)$ families

$$\lim_{x\to\infty} \frac{\{p : p \equiv a \bmod p,\ p \le x\}}{\{p : p \le x\}} = \frac{1}{\phi(m)}$$

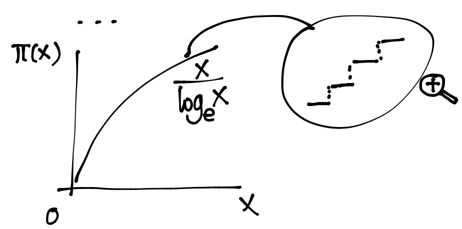
If $\gcd(a,m) > 1$, $p \equiv a \bmod m \Rightarrow \gcd(a,m) \mid p \Rightarrow \gcd(a,m) = p \Rightarrow p \mid m$. (so we need that precondition)

Chapter 13. $\pi(x) = \{p : p \le x\}$ counting function for primes

$\pi(10) = |\{2,3,5,7\}| = 4$

$\pi(5000) = 669$

. . .



$$\pi(x) \sim \frac{x}{\log_e x}$$

prime number theorem

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log_e x}} = 1$$

Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, $\mathrm{Re}|s| > 1$

$= \prod_p (1 - p^{-s})^{-1}$

Riemann Hypothesis $\Longleftrightarrow |\pi(x) - Li| < \frac{1}{8\pi} x^{\frac{1}{2}} \log x$

$Li = \int_2^x \frac{1}{\log t} dt \sim \frac{x}{\log x}$

Tenary Goldbach problem:

Every odd pos integer $\geqslant 7$ is a sum of 3 primes.

$7=2+3+3$

$9=3+3+3$

Goldbach problem:

Every even integer is a sum of 2 primes. (unsolved)

Twin prime conjecture: there are inifinite primes, p prime & p+2 is also a prime. (unsolved)

Prime gap: $\liminf_{n\to\infty} |P_m - P_n| < 7\times 10^7$ (Yitang Zhang)

< 600?

Counting function for twin prime:

$Twin(x) = \#\{\text{prime } p \leq X : p+2 \text{ is a prime}\}$

$$\lim_{x\to\infty} \frac{Twin(x)}{\frac{x}{(\log x)^2}} \doteq 0.66016$$

unsolved.

Counting function for N^2+1 form:

$P(x) = \#\{\text{prime } p \leq X : p \text{ is of the form } N^2+1\}$

$$\lim_{x\to\infty} \frac{P(x)}{\frac{\sqrt{x}}{\log x}} = C' \neq 0$$

Chapter 14 Mersenne Prime

Prime of the form 2^p-1. p is prime

Prime of the form a^n-1, $n\geqslant 2$

$31=2^5-1$

$\to$ divisible by $a-1$

it's not a prime unless $a=2$

so $2^n-1 \Rightarrow$ frequently a composite:

$2^9-1=7\times 73$

$2^{10}-1=3\times 11\times 31$

Claim: If $n=mk$, then 2^n-1 is divisible by 2^m-1

$$2^n-1=(2^m)^k-1=\underbrace{(2^m-1)}_{\text{factor}}((2^m)^{k-1}+\cdots+2^m+1)$$

so we prove the following: If a^n-1 is a prime for $a\geqslant 2$, $n\geqslant 2$, then $a=2$, n is a prime. (converse is not true)

For p prime: 2^p-1 may be not a prime
$2^{11}-1=2047=23\times 89$

Prime of the form 2^p-1 are called Mersenne prime.

Q: Infinitely many Mersenne prime? (unsolved).