PMATH 740 - Analytic Number Theory 2015 09 14

1. Prime Numbers

For $n \in \mathbb{N} = \{1, 2, 3, \dots\}$ let p_n be the n^{th} prime.
$p_1 = 2$, $p_2 = 3$, ...

Theorem 1 (Euclid). There are infinitely many primes.

Proof: Suppose that there are only finitely many primes, say $p_1, \dots, p_n$. Consider

$$m = p_1 p_2 \cdots p_n + 1 \geq 2.$$

By the fundamental theorem of arithmetic, m is a product of primes. Thus $p_k \mid m$ for some $k \in \mathbb{N}$ with $1 \leq k \leq n$. Then

$$p_k \mid (m - p_1 p_2 \cdots p_n) \quad \text{ie} \quad p_k \mid 1,$$

a contradiction. Thus, there are infinitely many primes. ∎

Def'n For $x \in \mathbb{N}$, let

$$\pi(x) := \#\{p \leq x ; p = \text{prime}\}.$$

By theorem 1, $\pi(x) \to \infty$ as $x \to \infty$.

Our goal is to know how "large" $\pi(x)$ is.

Proposition 2: For $n \in \mathbb{N}$, we have $p_n \leq 2^{2^n}$

Proof: We prove this result by induction. For $k=1$, we have

$$p_1 = 2 \leq 2^{2^1}.$$

Suppose that the result holds for $1 \leq k \leq n$. We have seen in the proof of theorem 1 that

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1.$$

Thus by induction hypothesis,

$$p_{n+1} \leq 2^{2^1} \cdots 2^{2^n} + 1 = 2^{2^{n+1}-2} + 1 \leq 2^{2^{n+1}}$$

By induction, the result holds. ∎

Corollary 3: For $x \in \mathbb{R}$ with $x \geq 2$, we have $\pi(x) \geq \log\log x$

Proof: (method 1): We first note that the result holds for $2 \leq x \leq 4$. For $x \geq 4$, let $s \in \mathbb{N}$ satisfy

$$2^{2^s} \leq x < 2^{2^{s+1}}.$$

By proposition 2, $x \geq 2^{2^s} \geq p_s \Rightarrow \pi(x) \geq s$. By taking logarithms twice,

$$x < 2^{2^{s+1}} \Rightarrow \log x < 2^{s+1} \log 2$$

$$\Rightarrow \frac{\log\left(\frac{\log x}{\log 2}\right)}{\log 2} < s+1$$

It follows that

$$\pi(x) \geq s > \frac{\log\left(\frac{\log x}{\log 2}\right)}{\log 2} - 1 > \log\log x. \quad \blacksquare$$

Proof: (method 2): Note that for all primes p, we have

$$\left(1 - \frac{1}{p}\right) \geq \frac{1}{2} \Rightarrow \left(1 - \frac{1}{p}\right)^{-1} \leq 2$$

Thus for $x \geq 2$,

$$2^{\pi(x)} \geq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)$$

$$\geq \sum_{n \leq x} \frac{1}{n}$$

$$\geq \int_1^x \frac{du}{u}$$

$$\geq \log x.$$

Thus

$$\pi(x) \geq \frac{\log\log x}{\log 2} \geq \log\log x. \quad \blacksquare$$

Fermat (1601-1655) conjectured that the numbers of the form

$$2^{2^n} + 1 \quad \text{for } n \in \mathbb{N} \cup \{0\}$$

are primes

He checked it for $n = 0,1,2,3,4$. These are known as the Fermat numbers and are denoted by F_n. In 1732, Euler proved that $641 \mid F_5$. It is known that $F_6, \dots, F_{21}$ are composite.

Theorem 4: (Pólya): For $n, m \in \mathbb{N}$ with $n \neq m$ we have $(F_n, F_m) = 1$.

Proof: Let $m = n+k$ with $k \in \mathbb{N}$.
Claim: $F_n \mid (F_m - 2)$
Verification: We have

$$F_m - 2 = \left(2^{2^{n+k}} + 1\right) - 2 = 2^{2^{n+k}} - 1$$

Write $x = 2^{2^n}$. Then

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x+1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1 \in \mathbb{N}$$

Thus the claim holds. □
Let $d = (F_n, F_m)$. Since $d \mid F_n$ and $d \mid F_m$. By the claim,

$$d \mid (F_m - 2) \Rightarrow d \mid 2.$$

Since $2 \nmid F_n$, we have $d = 1$. ■

Remark: From theorem 4, we obtain another proof of theorem 1 and proposition 2.

Theorem 5. For $x \geq 2$,

$$\pi(x) \geq \frac{\log x}{2 \log 2}.$$

Also, for $n \geq 1$, $p_n \leq 4^n$

Proof: Let $p_1, \dots, p_j$ be the primes at most x. For $n \in \mathbb{N}$ with $n \leq x$, write $n = n_1^2 m$ with $n_1 \in \mathbb{N}$ and m square-free,
ie $m = p_1^{\varepsilon_1} \cdots p_j^{\varepsilon_j}$ where $\varepsilon_i \in \{0,1\}$'s for each $i = 1, \dots, j$.
Thus, there are at most 2^j possible choices for m and at most $\sqrt{x}$ possible values for n_1. Thus

$$2^j \sqrt{x} \geq x \Rightarrow 2^j \geq \sqrt{x}. \quad \text{---} \quad (1)$$

Since $j = \pi(x)$, we have

$$\pi(x)\log 2 \geq \tfrac{1}{2}\log x$$
$$\Rightarrow \pi(x) \geq \frac{\log x}{2\log 2}$$

Also, if we take $x = p_n$, then $j = \pi(p_n) = n$. Then from (1),
$$2^n \geq \sqrt{p_n} \Rightarrow 4^n \geq p_n$$ ∎

In 1896, Hadamard and de la Vallée proved independently the prime number theorem. More precisely, they showed that
$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$
(conjectured by Gauss).

Let $n \in \mathbb{N}$ and p be prime. Then the exact power of p dividing $n!$ is
$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\lfloor \frac{\log n}{\log p} \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Theorem 6. For $x \geq 2$, we have
$$\left(\frac{3\log 2}{8}\right)\frac{x}{\log x} < \pi(x) < (6\log 2)\frac{x}{\log x}.$$

Proof (argument due to Erdös): Consider first a lower bound for $\pi(x)$. Note that the binomial coefficient
$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \in \mathbb{N}.$$

Claim: $$\binom{2n}{n} \Big| \prod_{p \leq 2n} p^{r_p}$$
where $r_p \in \mathbb{N} \cup \{0\}$ satisfies $p^{r_p} \leq 2n < p^{r_p+1}$.
Verification: Note that the exact power of p dividing $(2n)!$ is
$$\sum_{k=1}^{r_p} \left\lfloor \frac{2n}{p^k} \right\rfloor$$
and the exact power of p dividing $n!$ is
$$\sum_{k=1}^{r_p} \left\lfloor \frac{n}{p^k} \right\rfloor.$$
Thus the exact power of p dividing $\binom{2n}{n}$ is

2015 09 16 (2

$$\sum_{k=1}^{r_p} \Big(\underbrace{\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor}_{\leq 1} \Big) \leq r_p.$$

Thus the claim holds. □

From the claim,

$$\binom{2n}{n} \leq \prod_{p \leq 2n} p^{r_p} \leq (2n)^{\pi(2n)}.$$

Note that

$$\binom{2n}{n} = \frac{(n+1)\cdots(2n)}{1\cdots n} = \left(\frac{n+1}{1}\right)\left(\frac{n+2}{2}\right)\cdots\left(\frac{2n}{n}\right) \geq 2^n.$$

By the above two inequalities,

$$2^n \leq (2n)^{\pi(2n)}.$$

It follows that

$$\pi(2n) \geq \frac{n\log 2}{\log(2n)} = \left(\frac{\log 2}{2}\right)\frac{2n}{\log(2n)}.$$

Note that $\frac{x}{\log x}$ is increasing for $x \geq e$. For $x \geq 6$, let $n \in \mathbb{N}$ satisfy

$$\frac{3}{4}x < 2n \leq x.$$

Then

$$\pi(x) \geq \pi(2n) \geq \left(\frac{\log 2}{2}\right)\left(\frac{2n}{\log(2n)}\right) \geq \left(\frac{\log 2}{2}\right)\frac{\frac{3}{4}x}{\log\left(\frac{3}{4}x\right)} \geq \frac{3\log 2}{8}\,\frac{x}{\log x}.$$

We have checked that the lower bound holds for $x \geq 6$. It is easy to check for $2 \leq x \leq 6$. 2015 09 18

We now consider the upper bound. Note that

$$\prod_{n < p \leq 2n} p \;\Big|\; \binom{2n}{n}.$$

Thus

$$\prod_{n < p \leq 2n} p < (1+1)^{2n} = 2^{2n}.$$

On the other hand,

$$\prod_{n < p \leq 2n} p \geq n^{\pi(2n) - \pi(n)}$$

It follows that

$$n^{\pi(2n)-\pi(n)} \leq 2^{2n}.$$

Thus

$$\pi(2n)\log n - \pi(n)\log n < (\log 2)2n$$
$$\Rightarrow \pi(2n)\log n - \pi(n)\log\left(\tfrac{n}{2}\right) < (\log 2)2n + (\log 2)\pi(n) < (3\log 2)n.$$

Take $n = 2^k$. Then

$$\pi(2^{k+1})\log 2^k - \pi(2^k)\log 2^{k-1} < (3\log 2)2^k$$
$$\pi(2^k)\log 2^{k-1} - \pi(2^{k-1})\log 2^{k-2} < (3\log 2)2^{k-1}$$
$$\vdots$$
$$\pi(8)\log 4 - \pi(4)\log 2 < (3\log 2)4$$

It follows that

$$\pi(2^{k+1})\log 2^k < (3\log 2)(2^k + 2^{k-1} + \cdots + 4) + \pi(4)\log 2$$
$$< (3\log 2)2^{k+1} \qquad \text{(exercise)}$$

Thus

$$\pi(2^{k+1}) < (3\log 2)\left(\frac{2^{k+1}}{\log 2^k}\right)$$

For $x \geq 2$, let $k \in \mathbb{N}$ with $2^k < x \leq 2^{k+1}$. Then $\pi(x) \leq \pi(2^{k+1})$. Thus for $x \geq e$,

$$\pi(x) < (3\log 2)\frac{2^{k+1}}{\log 2^k} \leq (6\log 2)\frac{2^k}{\log 2^k} \leq (6\log 2)\frac{x}{\log x}$$

Also we can check that the upper bound holds for $2 \leq x \leq e$. ∎

In 1845, Bertrand showed that there is always a prime p in the interval $[n, 2n]$ for $n \in \mathbb{N}$ provided that $n < 6 \cdot 10^6$. He conjectured that this always holds. Chebyshev proved this in 1850.

Proposition 7: For $n \in \mathbb{N}$, we have

$$\prod_{p \leq n} p < 4^n.$$

Proof. We prove this result by induction. The claim holds for $n = 1$ and $n = 2$. Suppose that the result holds for $1 \leq k \leq (n-1)$. Since for $n \geq 2$, if n is even

$$\prod_{p \leq n} p = \prod_{p \leq (n-1)} p$$

we can consider only the case when n is odd. Write $n = 2m+1$ and

consider $\binom{2m+1}{m}$. We have

$$\prod_{(m+1)<p\le(2m+1)} p \;\Big|\; \binom{2m+1}{m}.$$

Note that $\binom{2m+1}{m}$ and $\binom{2m+1}{m+1}$ occur in the binomial expansion of $(1+1)^{2m+1}$ and $\binom{2m+1}{m}=\binom{2m+1}{m+1}$. Thus

$$\binom{2m+1}{m} \le \frac{1}{2}2^{2m+1} = 4^m.$$

By our induction hypothesis

$$\prod_{p\le(2m+1)} p = \left(\prod_{p\le(m+1)} p\right)\left(\prod_{(m+1)<p\le(2m+1)} p\right) \le 4^{m+1}\cdot 4^m = 4^n. \quad \blacksquare$$

For $\alpha\in\mathbb{N}\cup\{0\}$, we write $p^\alpha \| b$ to mean that $p^\alpha \mid b$ and $p^{\alpha+1}\nmid b$.

Proposition 8: If $n\ge 3$ and p is a prime with $\frac{2}{3}n<p\le n$, then

$$p\nmid\binom{2n}{n}$$

Proof: Since $n\ge 3$, if p satisfies $\frac{2n}{3}<p\le n$, then $p>2$. Thus p and $2p$ are the only multiples of p with $p\le 2n$, and so $p^2\|(2n)!$. Since $\frac{2n}{3}<p\le n$, we have $p\|n!$ and thus $p^2\|(n!)^2$. Since

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2},$$

we see that $p\nmid\binom{2n}{n}$. $\blacksquare$

Theorem 9 (Chebyshev): For $n\in\mathbb{N}$, there exists a prime p with $n<p\le 2n$.

Proof (argument due to Erdős): Note that the result holds for $n=1,2,3$. Suppose that the result is false for some $n\in\mathbb{N}$ with $n\ge 4$. Let p be a prime dividing $\binom{2n}{n}$ and $p^{\alpha_p}\|\binom{2n}{n}$. By our assumption, $p\le n$. Also, by proposition 8, $p\le\frac{2n}{3}$.
Let r_p be defined as in the proof of theorem 6, ie $p^{r_p}\le 2n<p^{r_p+1}$.
We have seen in the proof of theorem 6 that $\alpha_p\le r_p$. Thus

$$p^{\alpha_p}\le p^{r_p}\le 2n$$

If $\alpha_p\ge 2$ then $p^2\le 2n$, ie $p\le\sqrt{2n}$. By proposition 7 we have

$$\binom{2n}{n} \leq \left(\prod_{\substack{p \leq 2n \\ a_p \leq 1}} p\right)\left(\prod_{\substack{p \leq 2n \\ a_p \geq 2}} p^{a_p}\right) \leq 4^{\frac{2n}{3}} (2n)^{\pi(\sqrt{2n})}$$

$$\leq 4^{\frac{2n}{3}} (2n)^{\sqrt{2n}}$$

Note that $\binom{2n}{n}$ is the largest $(2n+1)$ terms in the binomial expression of

$$(1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n}.$$

Thus

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}.$$

Combining the above inequalities, we have

$$\frac{4^n}{2n+1} \leq 4^{\frac{2n}{3}} (2n)^{\sqrt{2n}} \Rightarrow 4^{\frac{n}{3}} \leq (2n)^{\sqrt{2n}} (2n+1) \leq (2n)^{\sqrt{2n}+2}.$$

Taking logarithms, we find that

$$\frac{n}{3} \log 4 < (\sqrt{2n} + 2) \log(2n).$$

By calculus (exercise), one can show the above inequality is false for $n \geq 512$. This implies that the statement of the theorem holds for $n \geq 512$. By checking all cases for $n < 512$, we see that the result holds for all $n \in \mathbb{N}$. ∎