Let

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$

for $x \geqslant 2$ be the "logarithmic integral" and $\pi(x) = \#\{p \in \mathbb{P} : 2 \leqslant p \leqslant x\}$. Consider the following data:

So $\pi(x) \risingdotseq \frac{x}{\log(x)}$ but $\pi(x) \risingdotseq \mathrm{Li}(x)$ is better, and $\frac{\pi(x)}{x} \to 0$ as $x \to 0$ apparently. Indeed $\pi(x) \sim \frac{x}{\log(x)} \sim \mathrm{Li}(x)$.

This distribution is the subject of the famous **Prime Number Theorem**, which took all of the 19th century to prove.

Because $\log(10^n) = n\log(10)$

$$\begin{array}{ll} \text{in } [2, 100] : & \text{about } \frac{1}{2} \text{ the numbers are prime} \\ \text{in } [2, 1000] : & \frac{1}{3} \\ \text{in } [2, 1,000,000] : & \frac{1}{6} \text{ etc.} \end{array}$$

so they progressively thin out with a *local density* $\frac{1}{\log(t)}$ since if $a < b$

$$\#\{p \in \mathbb{P} : a \leqslant p \leqslant b\} = \pi(b) - \pi(a) \sim \int_2^b \frac{dt}{\log t} - \int_2^a \frac{dt}{\log t} = \int_a^b \frac{dt}{\log(t)}.$$

Theorem 20 *For $n \geqslant 2$,*

$$\frac{1}{8} \leqslant \frac{\pi(n)}{n/\log n} \leqslant 12.$$

Note: This is as close as we will get to proving the Prime Number Theorem.

Lemma ***(Chebyshev)*** *If* $H(n) = \sum_{j=2}^{n} \frac{1}{j}$ *then*

$$\frac{1}{8} \leqslant \pi(n)\frac{H(n)}{n} \leqslant 6.$$

Proof. Proof of Theorem 20 assuming Chebychev's Lemma:

For $n \geqslant 2$,

$$\log\left(\frac{n}{2}\right) = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log(n)\,.$$

For $n \geqslant 4$,

$$\frac{1}{2}\log(n) \leqslant \log\left(\frac{n}{2}\right).$$

Hence $\frac{1}{2}\log(n) \leqslant H(n) \leqslant \log(n)$ so, by the RHS of Chebychev's Lemma,

$$\frac{\pi(n)\log(n)}{n} \leqslant \frac{\pi(n)\,2H(n)}{n} \leqslant 12$$

and by the LHS of Chebychev's Lemma

$$\frac{1}{8} \leqslant \frac{\pi(n)H(n)}{n} \leqslant \frac{\pi(n)\log(n)}{n}$$

using Lemma 2 when $n \geqslant 4$.

If $n = 2,\ \pi(2) = 1$ and

$$\frac{1}{8} \leqslant \underbrace{\frac{1}{2/\log(2)}}_{0.34} \leqslant 6.$$

If $n = 3,\ \pi(3) = 2$ and

$$\frac{1}{8} \leqslant \underbrace{\frac{2}{3/\log(3)}}_{0.73} \leqslant 6.$$

This completes the proof of the theorem.

Proof of Lemma 2:

$$\mathit{Claim} : \forall k \geqslant 0,\ \pi(2^{k+1}) \leqslant 2^k \tag{9}$$

Proof: If $x > 9,\ \pi(x) \leqslant \frac{x}{2}$ since all even numbers greater than 2 are composite. Since $\pi(2^1) = 1 = 2^0,\ \pi(4) = 2 = 2^1$ and $\pi(8) = r = 2^2$, (1) is true $\forall k \geqslant 0$.

$$\mathit{Claim} : \frac{1}{2}\ell \leqslant H(2^\ell) \leqslant \ell \tag{10}$$

where $H(n) = \frac{1}{2} + \cdots + \frac{1}{n}$.

$$\begin{aligned} H(2^\ell) &= \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^{\ell-1}+1} + \cdots + \frac{1}{2^\ell}\right) \\ &\geqslant \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^\ell} + \cdots + \frac{1}{2^\ell}\right) \\ &= \frac{\ell}{2} \end{aligned}$$

and

$$\begin{aligned} H(2^\ell) &= \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + \left(\cdots + \frac{1}{2^\ell}\right) \\ &\leqslant \left(\frac{1}{2} + \frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) + \cdots + \left(\frac{1}{2^{\ell-1}} + \cdots \frac{1}{2^{\ell-1}}\right) \\ &\leqslant \ell \end{aligned}$$

This proves the claim.

If $p \in \mathbb{P}$ has $n < p < 2n \;\Rightarrow\; p \,|\, 2n!$ and $p \nmid n! \;\Rightarrow$

$$p \;\Big|\; \binom{2n}{n} = \frac{2n!}{n!\,n!} \;\Rightarrow\; \prod_{n<p<2n} p \;\Big|\; \binom{2n}{n} \tag{11}$$

By Lagrange, the power of p in $\binom{2n}{n}$ is

$$\sum_{m=1}^{r}\left(\left\lfloor\frac{2n}{p^m}\right\rfloor-2\left\lfloor\frac{n}{p^m}\right\rfloor\right) \tag{12}$$

where $p^r \leqslant 2n < p^{r+1}$ and the sum is $\leq r$ since $\forall x,\ \lfloor 2x\rfloor - 2\lfloor x\rfloor \leqslant 1$ (See below). Hence

$$\binom{2n}{n} \,\Big|\, \prod_{p^r \leqslant 2n < p^{r+1}} p^r$$

By (11) and (12)

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leqslant 2n} p \leqslant \binom{2n}{n} \leqslant \prod_{p^r \leqslant 2n < p^{r+1}} p^r \leqslant (2n)^{\pi(2n)} \tag{13}$$

Now

$$\binom{2n}{n} \leqslant (1+1)^{2n} = 2^{2n}$$

and

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

so

$$2^n \leqslant \binom{2n}{n} \leqslant 4^n \tag{14}$$

Using LHS of (13) we get $n^{\pi(2n)-\pi(n)} < 2^{2n}$ and the RHS gives $2^n < (2n)^{\pi(2n)}$, $n \geqslant 1$. Now let $n = 2^k$, $k = 0, 1, 2, \ldots$ so these two inequalities translate to

$$2^{k(\pi(2^{k+1})-\pi(2^k))} \leqslant 2^{2^{k+1}}, \quad 2^{2^k} \leqslant 2^{(k+1)\pi(2^{k+1})}, \quad k \geqslant 0$$

or

$$k(\pi(2^{k+1}) - \pi(2^k)) \leqslant 2^{k+1}, \quad 2^k \leqslant (k+1)\pi(2^{k+1}). \tag{15}$$

Hence

$$\begin{aligned}(k+1)\pi(2^{k+1}) - k\pi(2^k) &= k(\pi(2^{k+1}) - \pi(2^k)) + \pi(2^{k+1}) \\ &\leqslant 2^{k+1} + \pi(2^{k+1}) \\ &< 2^{k+1} + 2^k \quad \text{by (9)} \\ &= 3 \cdot 2^k\end{aligned}$$

Apply this for $k = 0, 1, 2, \ldots, k$ and add ($\pi(2^0) = \pi(1) = 0$):

$$\Rightarrow (k+1)\pi(2^{k+1}) < 3(2^0 + 2^1 + \cdots + 2^k) < 3 \cdot 2^{k+1}. \tag{16}$$

By (15) and (16), $\forall k \geqslant 0$

$$\frac{1}{2}\frac{2^{k+1}}{k+1} \leqslant \pi(2^{k+1}) < 3\frac{2^{k+1}}{k+1}.$$

If $n \in \mathbb{N}$, $n > 1$ choose k so $2^{k+1} \leqslant n < 2^{k+2}$. By (10) ($\pi$ is increasing)

$$\pi(n) \leqslant \pi(2^{k+2}) < 3\frac{2^{k+2}}{k+2} \leqslant 6\frac{2^{k+1}}{H(2^{k+2})} \leqslant \frac{6n}{H(n)}$$

(H is increasing) and

$$\begin{aligned} \pi(n) \geqslant \pi(2^{k+1}) &\geqslant \frac{1}{2}\frac{2^{k+1}}{k+1} \\ &= \frac{1}{8}\frac{2^{k+2}}{\frac{1}{2}(k+1)} \\ &\geqslant \frac{1}{8}\frac{2^{k+2}}{H(2^{k+1})} \\ &\geqslant \frac{1}{8}\frac{n}{H(n)} \end{aligned}$$

$$\Rightarrow \frac{1}{8} \leqslant \frac{\pi(n)}{n/H(n)} \leqslant 6$$

as claimed. □

Ex $\forall x \in \mathbb{R},\ 0 \leqslant \lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1$

Proof.

$$\begin{aligned} \lfloor x \rfloor &\leqslant x &\Rightarrow 2\lfloor x \rfloor &\leqslant 2x \\ \text{and } 2\lfloor x \rfloor &\in \mathbb{Z} &\therefore 2\lfloor x \rfloor &\leqslant \lfloor 2x \rfloor \end{aligned}$$

so $0 \leqslant \lfloor 2x \rfloor - 2\lfloor x \rfloor$

If $x \in \mathbb{Z}$, then $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 2x - 2 \cdot x = 0 \leqslant 1$.

If $x \notin \mathbb{Z}$, $\exists n \in \mathbb{Z}$ so $n < x < n+1$ and $x = n+\frac{1}{2}+\varepsilon$ where $|\varepsilon| < \frac{1}{2}$. Then $2x = 2n+1+2\varepsilon$.

$$\begin{aligned} \lfloor 2x \rfloor &= \lfloor 2n+1+2\varepsilon \rfloor \\ &= 2n+1+\lfloor 2\varepsilon \rfloor \qquad \lfloor x \rfloor = n \\ &= 2n+1 \end{aligned}$$

Hence $\lfloor 2x \rfloor - 2\lfloor x \rfloor = (2n+1) - 2n = 1 \leqslant 1$. $\square$

Note we have used several times the result

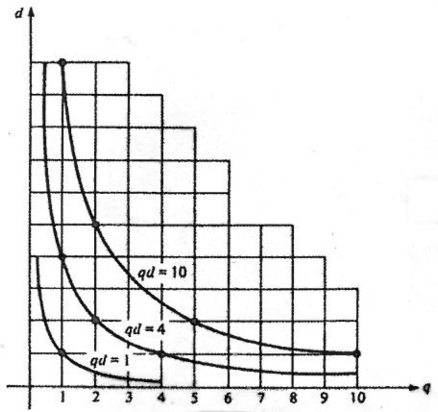
$$\lfloor y+n \rfloor = \lfloor y \rfloor + n \ \forall n \in \mathbb{Z}\,. \text{ (Ex)}$$

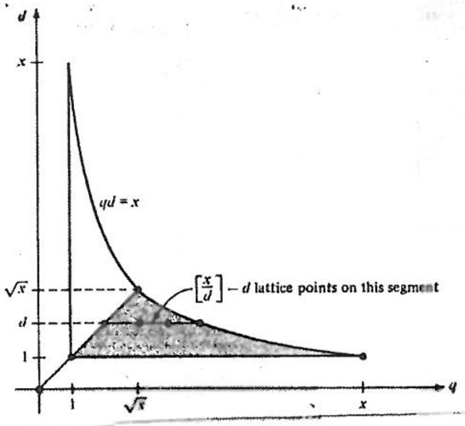
5 Primes in Gaps

- primes can be *close* together: $\{11, 13\}, \{29, 31\}, \{101, 103\}, \ldots$
- there can be *long* stretches of $\mathbb{N}$ with *no primes*:

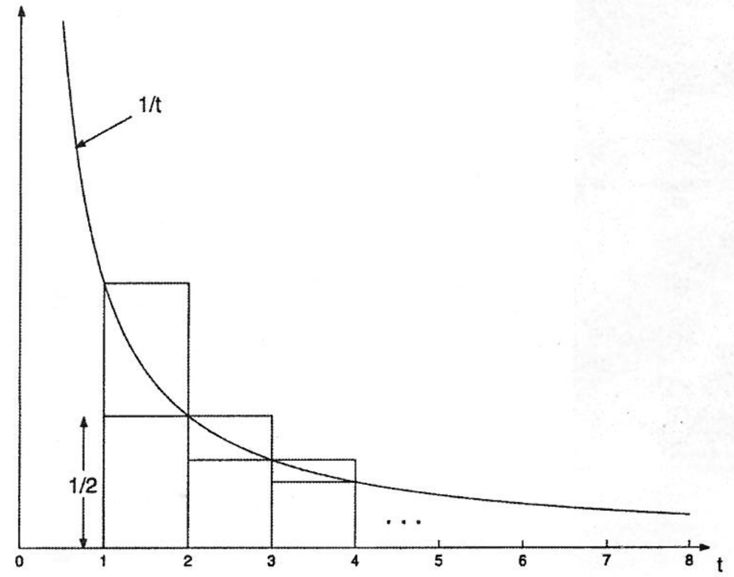
$$\left.\begin{array}{lcl} a_1 & = & n! + 2 \\ a_2 & = & n! + 3 \\ & \vdots & \\ a_{n-1} & = & n! + n \end{array}\right\} \begin{array}{c} \text{are } n-1 \text{ composite and consecutive} \\ \text{numbers, so none are prime} \\ \text{and } n \text{ can be as large as you like.} \end{array}$$

- we will prove the celebrated **Bertrand's Hypothesis**: $\forall n \in \mathbb{N},\ \exists p \in \mathbb{P}$ with $n \leqslant p < 2n$.
- $\forall n \in \mathbb{N}$ does there exist a $p \in \mathbb{P}$ with $n^2 < p < (n+1)^2$?


d
q
qd = 10
qd = 4
qd = 1
1 2 3 4 5 6 7 8 9 10


d
q
x
$\sqrt{x}$
d
1
1
$\sqrt{x}$
x
qd = x
$\left[\frac{x}{d}\right] - d$ lattice points on this segment

x	$\pi(x)$	$\frac{x}{\log x}$	$\mathrm{li}\, x$	$\frac{\pi(x)}{\mathrm{li}\, x}$	$\frac{\pi(x)}{x}$
1 000	168	145	178	0.94...	0.1680
10 000	1 229	1 086	1 246	0.98...	0.1229
50 000	5 133	4 621	5 167	0.993...	0.1026
100 000	9 592	8 686	9 630	0.996...	0.0959
500 000	41 538	38 103	41 606	0.9983...	0.0830
1 000 000	78 498	72 382	78 628	0.9983...	0.0785
2 000 000	148 933	137 848	149 055	0.9991...	0.0745
5 000 000	348 513	324 149	348 638	0.9996...	0.0697
10 000 000	664 579	620 417	664 918	0.9994...	0.0665
20 000 000	1 270 607	1 189 676	1 270 905	0.9997...	0.0635
90 000 000	5 216 954	4 913 897	5 217 810	0.99983...	0.0580
100 000 000	5 761 455	5 428 613	5 762 209	0.99986...	0.0576
1 000 000 000	50 847 478	48 254 630	50 849 235	0.99996...	0.0508



Primes in Gaps

by

Kevin A Broughan
University of Waikato
kab@waikato.ac.nz

John Butcher taught a course in number theory soon after being appointed to the University of Auckland and I was a student in that class. An abiding interest in prime numbers has been a result of this course. In this talk I will give the elementary proof of Erdős that there is a prime in every gap:

$$n \le p \le 2n$$

describe some large gaps and report on progress that has been made towards proving the difficult conjecture that there is a prime in every gap:

$$n^2 \le p \le (n+1)^2$$

as well, of course, as giving some numerical evidence for its potential correctness.

Gaps are consecutive composites: ㊵

```
[[4],
 [6],
 [8, 9, 10],
 [12],
 [14, 15, 16],
 [18],
 [20, 21, 22],
 [24, 25, 26, 27, 28],
 [30],
 [32, 33, 34, 35, 36],
 [38, 39, 40],
 [42],
 [44, 45, 46],
 [48, 49, 50, 51, 52],
 [54, 55, 56, 57, 58],
 [60],
 [62, 63, 64, 65, 66],
 [68, 69, 70],
 [72],
 [74, 75, 76, 77, 78],
 [80, 81, 82],
 [84, 85, 86, 87, 88],
 [90, 91, 92, 93, 94, 95, 96]]
```

← ⑦

Searching for early gaps:

㊶

g	$p(g)$	
456	25056082543	
464	42652618807	
468	127976335139	
474	182226896713	
486	241160624629	
490	297501076289	
500	303371455741	
514	304599509051	
516	416608696337	
532	461690510543	
534	614487454057	
540	738832928467	
582	1346294311331	
588	1408695494197	
602	1968188557063	
652	2614941711251	
674	7177162612387	
716	13829048560417	
766	19581334193189	
778	42842283926129	
804	90874329412297	← 1993

Aron, Potter, Young

$$\lim_{n\to\infty} [\text{size of gap } n] = \infty.$$

If $n \in \mathbb{N}$

$$\begin{aligned} a_1 &= (n+1)!+2 \\ a_2 &= (n+1)!+3 \\ a_3 &= (n+1)!+4 \\ &\vdots \\ a_n &= (n+1)!+(n+1) \end{aligned}$$

Then $\{a_1, \dots, a_n\}$ are consecutive and $i+1 \,|\, a_i \;\Rightarrow$ composite.

But [1993] best gap length $= 804$ at $p \approx 10^{15}$.

$n = 804 \;\Rightarrow\; n! \approx 0.771 \times 10^{1977}$.

Proof of Bertrand's Postulate

Proof. Claim:

$$x \geqslant 2 \;\Rightarrow\; \prod_{p \leqslant x} p \leqslant 4^{x-1} \tag{17}$$

If q is the largest prime less than or equal to x

$$\prod_{p \leqslant x} p = \prod_{p \leqslant q} p \text{ and } 4^{q-1} \leqslant 4^{x-1}$$

so we can assume $x = q$ is *prime*. If $q = 2$, $2 \leqslant 4^{2-1}$ so let $q = 2m+1$ be *odd*. Then

$$\begin{aligned} \prod_{p \leqslant 2m+1} p &= \left(\prod_{p \leqslant m+1} p\right) \cdot \left(\prod_{m+1 < p \leqslant 2m+1} p\right) \\ &= A \cdot B \end{aligned}$$

By induction $A \leqslant 4^m$. Also

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!\,(m+1)!}$$

so all primes in B divide the numerator and are *not cancelled* so

$$B \leqslant \binom{2m+1}{m} = \binom{2m+1}{m+1} \leqslant \frac{1}{2}(1+1)^{2m+1}$$

Hence $A \cdot B \leqslant 4^m 2^{2m} = 4^{2m+1-1} = 4^{x-1}$, which proves the claim.

Legendre's Theorem Implications

$n!$ contains the prime factor p exactly $\sum_{j\geqslant 1}\left\lfloor \frac{n}{p^{\alpha}} \right\rfloor$ times.

Ex $24! = 2^{22}\cdot 3^{10}\cdot 5^4\cdot 7^3\cdot 11^2\cdot 13\cdot 17\cdot 19\cdot 23$

$$p = 23: \left\lfloor \frac{24}{23} \right\rfloor = 1, \left\lfloor \frac{24}{23^2} \right\rfloor = 0, \cdots$$
$$p = 7: \left\lfloor \frac{24}{7} \right\rfloor = 3, \left\lfloor \frac{24}{7^2} \right\rfloor = 0, \cdots$$

Claim:

$$p^r \left| \binom{2n}{n} \right. \Rightarrow p^r \leqslant 2n.$$

$\binom{2n}{n}$ contains p $\sum_{j\geqslant 1}\left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2\left\lfloor \frac{n}{p^j} \right\rfloor\right)$ times. But

$$0 \leqslant \left\lfloor \frac{2n}{p^j} \right\rfloor - 2\left\lfloor \frac{n}{p^j} \right\rfloor < \frac{2n}{p^j} - 2\left(\frac{n}{p^j} - 1\right) = 2$$

$\Rightarrow$ each summand is 0 or 1 and is 0 for $p^j > 2n$

$$\Rightarrow \sum_{j\geqslant 1}\left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2\left\lfloor \frac{n}{p^j} \right\rfloor\right) \leqslant max\{j : p^j \leqslant 2n\}$$

$\Rightarrow$ if $p^2 > 2n$, p occurs at most once in $\binom{2n}{n}$.

If $\frac{2}{3}n < p \leqslant n \;\Rightarrow\; p$ does *not* appear in $\binom{2n}{n}$.

$\frac{2}{3}n < p \;\Rightarrow\; 2n < 3p \Rightarrow\; p, 2p$ are the only multiples of p in the numerator of $\frac{(2n)!}{n!\,n!}$.
$p \leqslant n \;\Rightarrow$ there are *two* in the denominator. So they *cancel.*

Ex $n = 24$

$$\binom{48}{24} = 2^2 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 41 \cdot 43 \cdot 47$$

$$\sqrt{2 \times 24} \qquad 16 < p \leqslant 24$$

Grand Finale

Assume that for some $n \in \mathbb{N}$ there is *no* p in $n < p < 2n$ (???). Now

$$\sum_{j=0}^{2n} \binom{2n}{j} = 2^{2n} \;\Rightarrow\; \binom{2n}{n} \geqslant \frac{4^n}{2n}$$

Hence

$$\frac{4^n}{2n} \leqslant \binom{2n}{n} \leqslant \overbrace{\left(\prod_{p \leqslant \sqrt{2n}} 2n\right)}^{A} \cdot \overbrace{\left(\prod_{\sqrt{2n} < p \leqslant \frac{2}{3}n} p\right)}^{B} \cdot \overbrace{\left(\prod_{n < p \leqslant 2n} p\right)}^{C}$$

$A \leqslant (2n)^{\sqrt{2n}}$, $C = 1$ by (???), $B \leqslant 4^{\frac{2}{3}n}$ by (17). Thus

$$4^n \leqslant (2n)^{1+\sqrt{2n}} 4^{\frac{2n}{3}}$$

$\Rightarrow \ \frac{n}{3}\log(4) \leqslant (1+\sqrt{2n})\log(2n) \ \Rightarrow \ n < 468.$

But $n < p < 2n \ \Leftrightarrow \ p_{n+1} < 2p_n$.

Consider the primes q_j

$$\{2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631\}$$

$q_{j+1} < 2q_j$ so Bertrand's Postulate is true for $n < 468$ (!!!), hence it is true $\forall n \geqslant 2$. $\square$

Prime Number Theorem Implications

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

or

$$\pi(x) = \frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right)$$

Number of primes in $(x, x(1+\varepsilon)]$, $\varepsilon > 0$, is

$$\pi(x + \varepsilon x) - \pi(x) = \frac{\varepsilon x}{\log(x)} + o\left(\frac{x}{\log(x)}\right) > 0 \quad \text{for } x \geqslant x_\varepsilon$$

$\Rightarrow$ $\exists p$ with $x < p \leqslant (1+\varepsilon)x$ Let $\varepsilon = 1$ $\Rightarrow$ $\forall n \geqslant N_2$ $\exists p$

$$n < p < 2n$$

Bertrand's Postulate
Chebyshev [1850]
Ramanujan
Erdös at age 19 years

Progress beyond Bertrand

$\exists\theta < 1$ with $\pi(x + x^\theta) - \pi(x) \sim \frac{x^\theta}{\log(x)}$

1930	Hoheisel	$\theta = 1 - \frac{1}{33{,}000} + \varepsilon \ (\forall \varepsilon > 0)$
1937	Ingham	$\theta = \frac{5}{8} + \varepsilon$
1961	Montgomery	$\theta = \frac{3}{5} + \varepsilon$
1972	Huxley	$\theta = \frac{7}{12} + \varepsilon$
1979	Iwaniec, Jutlia	$\theta = \frac{13}{23} + \varepsilon$
1984	Iwaniec, Printz	$\theta = \frac{1}{2} + \frac{1}{21} + \varepsilon = 0.547\ldots + \varepsilon$
1994	Lou and Yeo	$\theta = \frac{7}{13} + \varepsilon = 0.538\ldots + \varepsilon$
1998	Baker and Herman	$\theta = 0.535\ldots + \varepsilon$

Exercise for John in his Retirement

[Hardy and Wright, 1979]: There is a prime p with $n^2 < p < (n+1)^2$

Note: $\theta = \frac{1}{2} \ \Rightarrow \ \exists p \ x < p < x + \sqrt{x}$.
$x = n^2 \ \Rightarrow \ n^2 < p < n^2 + n < (n+1)^2$.

Degree of difficulty for the student:

Other Results on the Distribution of Primes

Theorem 21 (Bertrand's Postulate) $\forall n \in \mathbb{N},\ \exists p \in \mathbb{P}$ *with* $n \leqslant p < 2n$.

Theorem 22 *There are infinitely many primes of the form* $4n-1$.

Proof. Assume there are only a finite number and let p be the largest. Let

$$N = 2^2 \cdot \overbrace{3 \cdot 5 \cdots p}^{n} - 1$$

The product $n = 3 \cdot 5 \cdots p$ contains all the odd primes less than or equal to p as factors. Since $N > p$ and $N = 4n-1$, it cannot be prime. No prime less than or equal to p divides N (since it would divide 1). Thus all the prime factors of N must exceed p.

If $x = 4m+1$ and $y = 4\ell + 1$ then

$$xy = 16m\ell + 4m + 4\ell + 1 = 4(4m\ell + m + \ell) + 1 = 4k + 1$$

If two factors of N are of the form $4n+1$, so is their product. But N has the form $4n-1$, so at least one prime factor must be of the form $p = 4m-1$. This contradiction proves the theorem. ☐

Can also show there are an infinite number of primes of each of the forms $4n+1$, $5n-1$, $8n-1$, $8n-3$ and $8n+3$.

Note All numbers of the form $4n$ or $4n+2$ are composite. Every prime $p \in \mathbb{P}$ is of the form $4n+1$ or $4n+3$.

Theorem (Dirichlet) *If* $k > 0$ *and* $(h,\ k) = 1$ *then* $\forall x > 1$,

$$\sum_{\substack{p \leqslant x \\ p \equiv h \pmod{k}}} \frac{\log(p)}{p} = \frac{1}{\phi(k)} \log(x) + O(1)$$

Corollary *Since* $x \to \infty \ \Rightarrow \log(x) \to \infty$, *there are an infinite number of primes in every arithmetic progression* $nk + h$, $n = 0, 1, 2, 3, \ldots$ *since* $p = nk + h$ *for some* $n \Leftrightarrow p \equiv h \pmod{k}$.

Theorem (Dirichlet) *Let*

$$\pi_h(x) = \sum_{\substack{p \leqslant x \\ p \equiv h \pmod{k}}} 1.$$

Then $\pi_h(x)$ *counts the number of primes in* $nk + h$, $n = 0, 1, 2, 3, \ldots$.

$$\pi_h(x) \sim \frac{\pi(x)}{\phi(k)} \sim \frac{1}{\phi(k)} \frac{x}{\log(x)} \text{ as } x \to \infty$$

Corollary *For each* $h \pmod{k}$, $\pi_h(x)$ *has the same asymptotic value i.e. the number of primes in each class* $[\,h\,]_k$ *is asymptotically the same.*

Note All attempts to extend this result to more complex subsets of $\mathbb{N}$ than arithmetic progressions have *failed*.

1. Are there an infinite number of primes of the form $p = n^2 + 1$?

   Ex There are an infinite number of composites $xy = n^2 + 1$.

2. Are there an infinite number of primes p such that $q = 2p+1$ is also prime? (Sophie Germain primes.)

3. Are there an infinite number of primes p such that $q = p + 2$ is also prime? (Twin primes conjecture.)

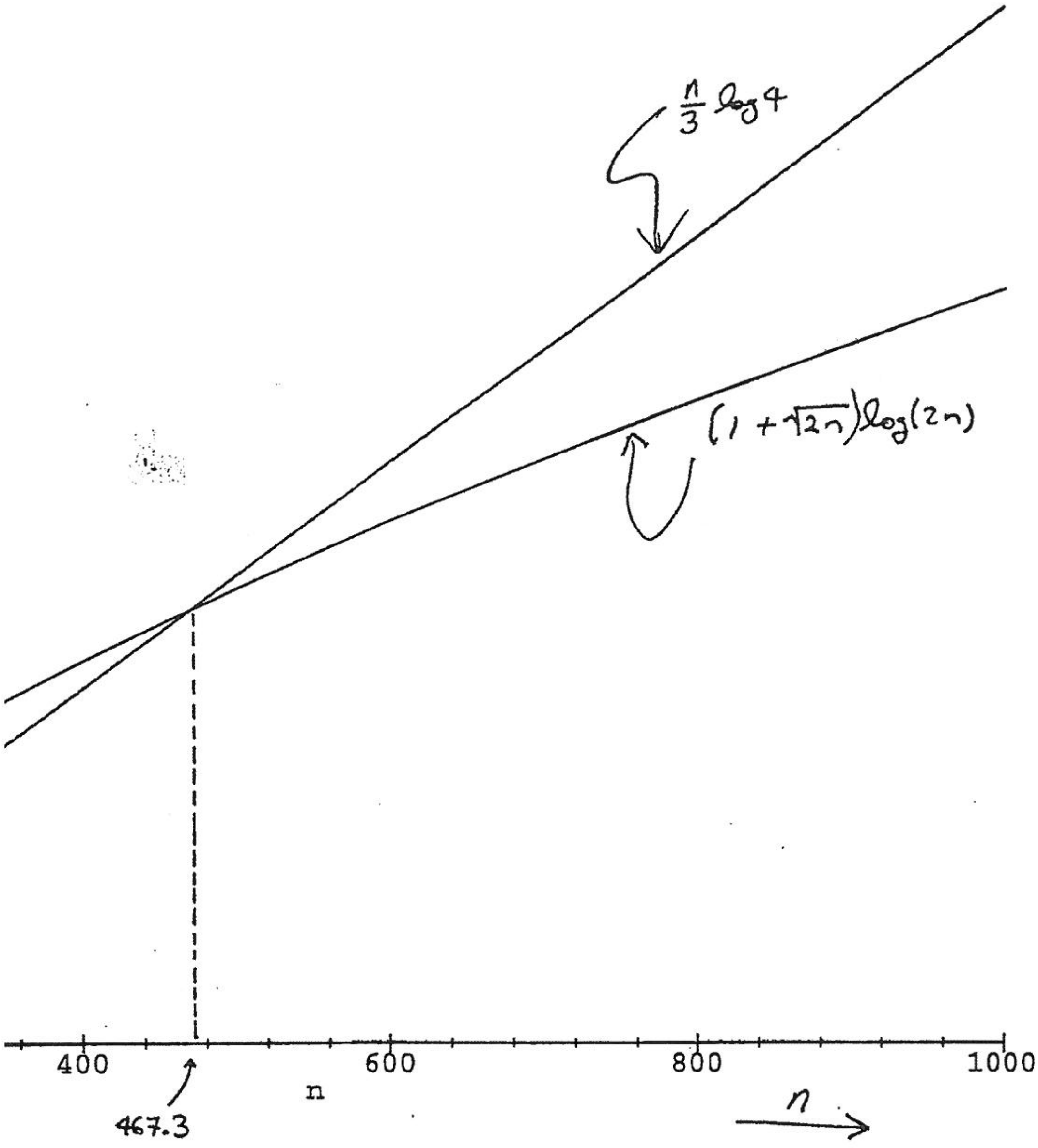
   Ex If $n > 3$ one of $\{n,\ n+2,\ n+4\}$ is divisible by 3, and is hence composite. (No triple primes conjecture.)

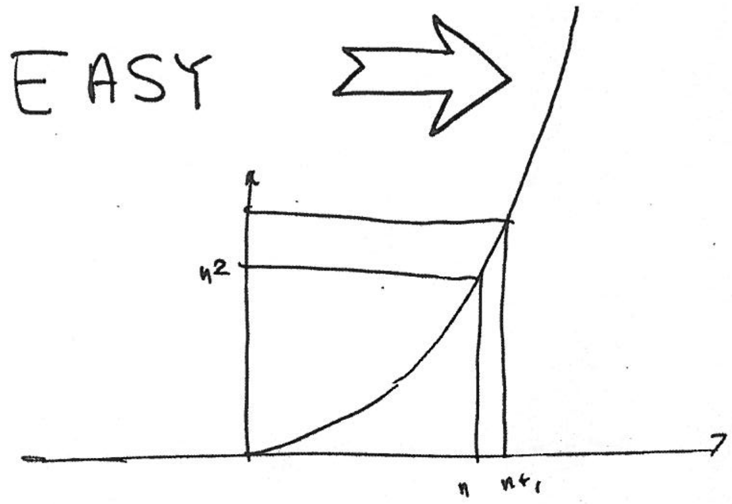
   Proof.

   $$\begin{aligned} n &\equiv 0 \pmod 3 & & & &\Rightarrow 3 \mid n \\ n &\equiv 1 \pmod 3 &\Rightarrow\ & n+2 \equiv 3 \equiv 0 \pmod 3 & &\Rightarrow 3 \mid n+2 \\ n &\equiv 2 \pmod 3 &\Rightarrow\ & n+4 \equiv 6 \equiv 0 \pmod 3 & &\Rightarrow 3 \mid n+4 \end{aligned}$$

   □

4. Find a *quadratic polynomial* $f(n) = an^2 + bn + c$ with an *infinite number* of prime values.


$\frac{n}{3}\log 4$
$(1+\sqrt{2n})\log(2n)$
400
600
800
1000
n
467.3
$n \rightarrow$


EASY
n^2
n
$n+1$

$$f(n) = \pi\left((n+1)^2\right) - \pi\left(n^2\right)$$