Notes on Pollack's "Not Always Buried Deep"

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: July 9, 2017)

Abstract

This is one of the best books on analytic number theory I've found to date. The comments here will be based on his notes with the same title instead of the book because the notes is free while the book is not :)

Page 3. On *Euclid's second proof*. The trick here is to show that $\varphi(P) > 1$, one thing to note is that $\varphi(n)$ measures the number of numbers that are co-prime to n. Since $\varphi(P) > 1$, there is a number that is co-prime to P but in that case that number must contain a new prime. The other details were to make sure there is such a co-prime number.

Page 4. This is really clever, first let's do induction to show that $n_i = 2^{2^{i-1}} + 1$. For $i = 1$ this is obvious as $3 = 2^{2^0} + 1$ we just need to show the induction hypothesis is true, say $n_i = 2^{2^{i-1}} + 1$ we need to show the same holds for n_{i+1}

$$\begin{aligned} n_{i+1} &= 2 + \prod_{1 \le j < i+1} n_j \\ &= 2 + n_i \prod_{1 \le j < i} n_j \\ &= 2 + n_i(n_i - 2) \\ &= 2 - 2n_i + n_i^2 \\ &= (n_i - 1)^2 + 1 \\ &= 2^{2^i} + 1 \end{aligned}$$

Next we tackle the claim that this upper bound on p_n gives us a lower bound on $\pi(x)$. Start with

$$\begin{aligned} p_i &< n_i \\ &< 2^{2^{i-1}} + 1 \\ &< 2^{2^{\pi(p_i)-1}} + 1 \\ \log\log(p_i) &< \pi(p_i) \end{aligned}$$

where there will be some very small correction terms due to the constant in the exponent and the one outside and of course due to the fact that we are using natural log instead of $\log_2$.

Page 5. Top of page, "the order of 2 (mod p) is precisely 2^i", why is this so? Why can't the order be smaller than 2^i, this is because

$$2^{2^i} = \left(\left((2)^2\right)^2\right)^2 \ldots$$

so we are just squaring over and over again, and since $2^{2^{i-1}} \equiv -1$ this means that there's no lower exponent that produces $+1$ otherwise $2^{2^{i-1}}$ wouldn't have been -1.

Next we tackle the comment that "$a_n = 2^n - 1$ has the desired properties (note that $a_{11} = 23 \cdot 89$)." The problem is when $n = 13$ which is also a prime $2^{13} - 1 = 8191$ which is a prime, it even fails for $2^5 - 1 = 31$, in hindsight, this is obvious since there are things called the Mersenne primes of the form $2^n - 1$:)

I then tried changing it to $a_n = 2^n + 1$ but it fails for $n = 3$ as $a_3 = 9$ and it doesn't have two distinct prime divisors but it's more promising, what we need is that $2^{2j+1} + 1$ to have more than 1 prime divisor, we know that $2^{2j+1} + 1$ is always a multiple of 3, it's obvious when you do (mod 3) as $2 \equiv -1 \pmod 3$.

The question now is if there will be a k such that $3^k = 2^{2j+1} + 1$, well for $j = 1$ we have $3^2 = 2^3 + 1$ so how about for $j > 1$?

Suppose we find a k such that $3^k = 2^{2j+1} + 1$, since $j > 1$, $4|2^{2j+1}$ and so by modulo 4 we know that k is even since $3 \equiv -1 \pmod 4$, so we can denote $k = 2m$

$$3^{2m} = 2^{2j+1} + 1$$
$$3^{2m} - 1 = 2^{2j+1}$$

Focusing on the LHS

$$\begin{aligned} 3^{2m} - 1 &= (3-1)(3^{2m-1} + 3^{2m-2} + 3^{2m-3} + 3^{2m-4} + \cdots + 3 + 1) \\ &= 2(3^{2m-2}(3+1) + 3^{2m-4}(3+1) + \cdots + (3+1)) \\ &= 2^3(3^{2m-2} + 3^{2m-4} + \cdots + 1) \end{aligned}$$

Now there are m terms inside the brackets in the RHS, if m is odd then

$$3^{2m-2} + 3^{2m-4} + 3^{2m-6} + 3^{2m-8} + \cdots + 1 = (3^{2m-2} + 3^{2m-4}) + (3^{2m-6} + 3^{2m-8}) + \cdots + 1$$

Each bracket in the RHS is even and so the total is odd and thus

$$3^{2m} - 1 = 2^3(2M + 1)$$

and it can't be 2^{2j+1} since $(2M + 1)$ is odd. Now if m is even we get

$$\begin{aligned} 3^{2m-2} + 3^{2m-4} + 3^{2m-6} + 3^{2m-8} + \cdots + 3^2 + 1 &= 3^{2m-4}(3^2+1) + 3^{2m-8}(3^2+1) + \cdots + (3^2+1) \\ &= 2 \cdot 5(3^{2m-4} + 3^{2m-8} + \cdots + 1) \end{aligned}$$

but 5 is prime and so $3^k - 1$ can't be 2^{2j+1}. Therefore $2^{2j+1} + 1$ contains at least two prime divisors for $j > 1$ only for $j = 1$ does it contain only one prime divisor.

But we cannot use $a_n = 2^n + 1$ for the proof in the book, because then each a_n is a multiple of 3 and they are not co-prime.

The proof in the book still works even is we use $a_n = 2^n - 1$ as long as we include $n = 11$ because then $a_2a_3a_5a_7a_{11}$ still have $5 + 1$ prime factors, note that a_2, a_3, a_5, a_7 are all prime numbers.

Exercise 1.2.3. **Page 5**. We are given

$$n_i = 1 + \prod_{j<i} n_j$$

a) Prove that n_i are pairwise relatively prime. Suppose we have any two $n_{a,b}$ with $a < b$ and $d = \gcd(n_a, n_b)$ then

$$\begin{aligned} n_b &= 1 + \prod_{j<b} n_j \\ &= 1 + n_a \prod_{j<b, j\neq a} n_j \\ n_b - n_a \prod_{j<b, j\neq a} n_j &= 1 \\ d\left(n'_b - n'_a \prod_{j<b, j\neq a} n_j\right) &= 1 \\ d &\mid 1 \end{aligned}$$

b) Show that $n_i = f(n_{i-1})$ where $f(T) = T^2 - T + 1$

$$\begin{aligned} n_i &= 1 + \prod_{j<i} n_j \\ &= 1 + n_{i-1} \prod_{j<i-1} n_j \\ &= 1 + n_{i-1}(n_{i-1} - 1) \\ &= n_{i-1}^2 - n_{i-1} + 1 \end{aligned}$$

c) If $p|f(n)$ for some integer n, then -3 is a square (mod p). Taking a prime divisor of each n_i, conclude that there are innitely many primes $p \equiv 1 \pmod 3$.

For the first part p need not be prime.

$$\begin{aligned} T^2 - T + 1 = f(n) &= pf' \\ &\equiv 0 \pmod{p} \\ \rightarrow T &\equiv \frac{1 \pm \sqrt{-3}}{2} \end{aligned}$$

so for T to have a solution -3 must be a quadratic residue modulo p but we know that there's a solution which obviously is $T = n$ since $p = f(n)$.

For the second part we need p to be prime and we will utilize the quadratic reciprocity formula

$$\begin{aligned} \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) &= (-1)^{\frac{3-1}{2}\frac{p-1}{2}} \\ &= (-1)^{\frac{p-1}{2}} \\ \rightarrow \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} \\ \left(\frac{-3}{p}\right)\left(\frac{p}{3}\right) &= (-1)^{p-1}, \qquad p \text{ is prime, } p-1 \text{ is even} \\ (+1)\left(\frac{p}{3}\right) &= +1 \end{aligned}$$

So we know that p is a quadratic residue modulo 3, by Euler's theorem

$$\begin{aligned} p^{\frac{3-1}{2}} &\equiv 1 \pmod{3} \\ p &\equiv 1 \pmod{3} \end{aligned}$$

which is what we want

Exercise 1.2.4. **Page 5**. Let m be a positive integer. Let A_1 be any integer with $\gcd(A_1, m) = 1$, and for $n \geq 1$ dene

$$A_{n+1} = A_n^2 - mA_n + m.$$

a) Show that $\gcd(A_i, A_j) = 1$ for $i \neq j$. Suggestion: Show that if $p|A_i$ for some i, then for all $j > i$ we have $p \nmid A_j$.

There are a few things we can gather from the recurrence formula, first $\gcd(A_i, m) = 1$

for all i

$$\begin{aligned} A_2 &= A_1^2 - mA_1 + m \\ A_2 + m(A_1 - 1) &= A_1^2 \\ d(A_2' + m'(A_1 - 1)) &= A_1^2 \\ &\rightarrow d \mid A_1 \end{aligned}$$

but this means that $\gcd(A_1, m) = d$ but since these two are co-prime $d = 1$, we can repeat the process with A_2 and A_3 and so on, so by induction all A_i are co-prime to m.

Next, using the above result we can show that $\gcd(A_i, A_{i+1}) = 1$, by the same token

$$\begin{aligned} A_{i+1} &= A_i^2 - mA_i + m \\ A_{i+1} - A_i(A_i - m) &= m \\ d(A_{i+1}' - A_i'(A_i - m)) &= m \\ &\rightarrow d \mid m \end{aligned}$$

but we know that the A's are co-prime to m so $d = 1$. Inspired by this we can go further

$$\begin{aligned} A_{i+2} &= A_{i+1}^2 - mA_{i+1} + m \\ &= (A_i^2 - mA_i + m)^2 - m(A_i^2 - mA_i + m) + m \\ &= A_iK + m^2 - m^2 + m \\ &= A_iK + m \end{aligned}$$

where K contains all cross terms betwen A_i and m, we can of course repeat this process

$$\begin{aligned} A_{i+3} &= A_{i+2}^2 - mA_{i+2} + m \\ &= (A_iK + m)^2 - m(A_iK + m) + m \\ &= A_iK' + m^2 - m^2 + m \\ &= A_iK' + m \end{aligned}$$

and so on, now say we choose two $A_{i,j}$ with $i < j$ then by the process above we will get

$$\begin{aligned} A_j &= A_i K''' + m \\ \rightarrow A_j - A_i K''' &= m \\ d(A'_j - A'_i K''') &= m \\ d &\mid m \end{aligned}$$

but from our previous result every A is co-prime to m and so $d = 1$ which means that the A are pairwise co-prime.

b) Show that if $A_1 > m$, one has $A_n > m \geq 1$ for every n. Use this to give another demonstration that there are an innite number of primes.

Since $A_1 > m$, $A_1^2 - mA_1 = A_1(A_i - m) > A_1$ and so $A_2 = A_1(A_1 - m) + m > A_1 + m > A_2$ and of course $A_2 > m$ also. Continuing this trend we have $A_{n+1} > A_n$.

c) Taking $A_1 = 3$ and $m = 2$, show that $A_n = 2^{2^{n-1}} + 1$; thus we have recovered Goldbachs proof. Note that the choice $A_1 = 2$, $m = 1$ corresponds to Exercise 1.2.3.

The choice of $A_1 = 3$ and $m = 2$ means that

$$\begin{aligned} A_2 &= A_1^2 - 2A_1 + 2 \\ &= (A_1 - 1)^2 + 1 \\ &= 2^2 + 1 \\ &= 2^{2^{2-1}} + 1 \end{aligned}$$

so we have the base case, inductively

$$\begin{aligned} A_{n+1} &= A_n(A_n - 2) + 2 \\ &= (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) + 2 \\ &= 2^{2^n} - 1 + 2 \\ &= 2^{2^n} + 1 \end{aligned}$$

while for $A_1 = 2$ and $m = 1$ we have $A_{n+1} = A_n^2 - A_n + 1 = f(A_n)$ where $f(T) = T^2 - T + 1$ as given in the previous problem.

The proofs of part (a) and (b) also work for $A_{n+1} = A_n^k - m^{k-j} A_n^j + m$

Exercise 1.2.5. **Page 6**. (Harris [Har56]). Let b_0, b_1, b_2 be positive integers with b_0 co-prime to b_2. Define A_k for $k = 0, 1$ and 2 as the numerator when the finite continued fraction

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots_{+\frac{1}{b_k}}}}$$

is put in lowest terms. For $k = 3, 4, \ldots$, inductively define b_k and A_k by $b_k = A_0 A_1 \ldots A_{k-3}$ and A_k by the rule given above. Prove that the A_i form an increasing sequence of pairwise coprime positive integers.

This one is a bit confusing, if I understand it correctly, the rules say that

$$A_0 = b_0$$

and

$$\begin{aligned} b_0 + \frac{1}{b_1} &= \frac{b_0 b_1 + 1}{b_1} \\ \rightarrow A_1 &= b_0 b_1 + 1 \end{aligned}$$

and finally

$$\begin{aligned} b_0 + \frac{1}{b_1 + \frac{1}{b_2}} &= b_0 + \frac{b_2}{b_1 b_2 + 1} \\ &= \frac{b_0 b_1 b_2 + b_2 + b_0}{b_1 b_2 + 1} \\ \rightarrow A_2 &= b_0 b_1 b_2 + b_2 + b_0 \end{aligned}$$

One attempt is to use partial convergents by way of ent.pdf, a finite continued fraction denoted as $[b_0, b_1, \ldots, b_k]$ can be expressed as p_k/q_k where

$$\begin{array}{llllll} p_{-2} = 0, & p_{-1} = 1, & p_0 = b_0, & p_n = b_n p_{n-1} + p_{n-2} & \ldots \\ q_{-2} = 1, & q_{-1} = 0, & q_0 = 1, & q_n = b_n q_{n-1} + q_{n-2} & \ldots \end{array}$$

And so $A_k = p_k = b_k A_{k-1} + A_{k-2}$, we will ignore the fact that we need to put the fraction p_k/q_k into its lowest terms for now, the first few A_k are

$$\begin{aligned} A_2 &= b_2 A_1 + A_0 \\ A_3 &= b_3 A_2 + A_1 = A_0 A_2 + A_1 \\ A_4 &= b_4 A_3 + A_2 = A_0 A_1 A_3 + A_2 \\ A_5 &= b_5 A_4 + A_3 = A_0 A_1 A_2 A_4 + A_3 \end{aligned}$$

Let's start with A_1 and A_0, since $A_0 = b_0$ and $A_1 = b_0 b_1 + 1$ they are obviously co-prime. Next, if A_2 is not co-prime to A_1 then

$$\begin{aligned} d(A_2' - b_2 A_1') &= A_0 \\ d \;&|\; A_0 \end{aligned}$$

not allowed since $(A_1, A_0) = 1$, by the same token if $(A_2, A_0) > 1$ then

$$\begin{aligned} d(A_2' - A_0') &= b_2 A_1 \\ d \;&|\; b_2 A_1 \end{aligned}$$

from above $(A_0, A_1) = 1$ so $d|b_2$, but $A_0 = b_0$ and $(b_0, b_2) = 1$ and since d divides both b_0 and b_2, d has to be 1. So we know that $(A_0, A_1) = (A_0, A_2) = (A_1, A_2) = 1$, following the same pattern we show that $(A_3, A_i) = 1$, $i < 3$, if $(A_3, A_{0,2}) > 1$, then $d|A_1$ but $A_{0,1,2}$ are all co-prime this shows that $A_{0,2,3}$ are co-prime, and the reverse is also true, if $(A_3, A_1) > 1$ then $d|A_{0,2}$ but we know that $A_{0,1,2}$ are all co-prime, so $A_{0,1,2,3}$ are all co-prime, and the same argument applies for all other A_k. In short all of the A_k are pairwise co-prime.

Now about the fraction being expressed in its lowest terms, one reason we need this is because we can always multiply numerator and denominator with any number we want so for example if we multiply A_0 by A_1/A_1 then A_0 will obviously not be co-prime to A_1. The only thing I'm not sure about is if the A_k will form an increasing sequence, this is because once put in the lowest term we divide out some factors. So we actually need not the lowest form requirement, we just need $A_k = p_k$, *i.e.* to be equal to the partial convergent.

Exercise 1.2.6. **Page 6**. Again, I'm not quite sure what it wants, does it mean the number of primes in the interval goes to infinity as r goes to infinity? but isn't it a circular argument? recall that r is the index of the r^{th} prime, by taking $r \to \infty$ we already assume that there are infinitely many primes ¯\(°_o)/¯ in any case ...

Page 9. Mid page-ish, "Proceeding as above, we deduce that $\sum_{p \le x} (p-1)^{-1} \ge \log\log x$", it's very tempting to just do log on both sides of (1.4) since the RHS is al-

ready $\log x$ but this will lead to some messy situation, salvageable but messy

$$\log\left(\prod_{p\le x}\frac{1}{1-\frac{1}{p}}\right)\ge\log\log x$$
$$\sum_{p\le x}\log\left(\frac{p}{p-1}\right)\ge\log\log x$$

We can still proceed by showing that

$$\frac{1}{p-1}>\log\left(\frac{p}{p-1}\right)$$

One way to show this is to show $\frac{1}{x-1}>\log\left(\frac{x}{x-1}\right)$ instead with all real number $x\ge 2$ (we choose 2 as the starting point for simplicity).

Well we know that at $x=2$, $\frac{1}{2-1}>\log\left(\frac{2}{2-1}\right)$, we now show that the slope for $\frac{1}{x-1}$ is always smaller to that of $\log\left(\frac{x}{x-1}\right)$ for all x and so $\frac{1}{x-1}>\log\left(\frac{x}{x-1}\right)$ always holds (we need a smaller slope because the function is a decreasing one).

The slope for $\frac{1}{x-1}$ is

$$\frac{d}{dx}\left(\frac{1}{x-1}\right)=-\frac{1}{(x-1)(x-1)}$$

while for $\log\left(\frac{x}{x-1}\right)$

$$\frac{d}{dx}\left(\log\left(\frac{x}{x-1}\right)\right)=-\frac{1}{x(x-1)}$$

and so the slope for $\frac{1}{x-1}$ is indeed smaller than that of $\log\left(\frac{x}{x-1}\right)$ and so $\frac{1}{x-1}>\log\left(\frac{x}{x-1}\right)$, this is one way.

Another way to show that $\sum_{p\le x}(p-1)^{-1}\ge\log\log x$ is to go back to the top of Page 9

$$\begin{aligned}\prod_{p\le x}\frac{1}{1-\frac{1}{p}}&=\prod_{p\le x}\left(1+\frac{1}{p-1}\right)\\&\le\prod_{p\le x}e^{1/(p-1)}=e^{\sum_{p\le x}(p-1)^{-1}}\end{aligned}$$

Combining all the inequalities (the one involving $\log x$ is from (1.4))

$$\log x\le\prod_{p\le x}\frac{1}{1-\frac{1}{p}}\le e^{\sum_{p\le x}(p-1)^{-1}}$$

taking the logarithm of both the far LHS and far RHS we have

$$\log\log x \leq \sum_{p\leq x}(p-1)^{-1}$$

which is what we want to show in the first place.

Page 11. There's a simple mistake on *J. Perott's proof*, "by removing those divisible by $1^2\ldots$", we cannot remove numbers divisible by 1^2 because then we will remove every number :)

Page 12. On J. Perott's proof, top of page, "It follows that $A(N)/N$ is bounded below $\ldots$ so the squarefree numbers have positive lower density", what it all means is that since $A(N)/N$ has a lower bound, if there are only a finite number of squarefree numbers then after a while (once we've passed the last one) $A(N)/N$ will get smaller and smaller and eventually gets smaller than the lower bound which is not allowed :)

Page 13. First paragraph, the conclusion of Erdos's super smart proof, "But $C\sqrt{N} < N/2$ whenever N is large", the question is so what? we know that $C\sqrt{N}$ is the number of integers $\leq N$ whose prime factors $\leq M$. The problem here is that we know that from page 12, the number of integers $\leq N$ whose prime factors $> M$ is $< N/2$, so the total number of integers (those with prime factors $\leq M$ + those with prime factors $> M$) must be N but here we have $< N/2 + < N/2$ which can never reach N

Exercise 1.2.7. **Page 9**. It's interesting that removing $\sum_p 1/p$ from $\sum_n 1/n$ makes the latter a convergent series. The question now is what is the minimum amount we need to subtract from $\sum_n 1/n$ to make it convergent?

Anyway, what we want to show is that $\sum_n 1/n$ with only *squarefull* n converges. We start with

$$\prod_p \left(1+\frac{1}{p^2}+\frac{1}{p^3}+\ldots\right) = \prod_p \left(\frac{1}{1-\frac{1}{p}}\right) - \frac{1}{p}$$

i.e. we remove the $1/p$ term from each series. Note that 1 is a squarefull number because the statement is that if $p|n$ then $p^2|n$ is a must, but for 1 no p divides 1 so it is considered squarefull a well. We then follow the same method as shown on Page 9

$$\prod_p \left[\left(\frac{1}{1-\frac{1}{p}}\right) - \frac{1}{p}\right] = \prod_p \left(1+\frac{1}{p-1}-\frac{1}{p}\right) = \prod_p \left(1+\frac{1}{p(p-1)}\right)$$

Now note that $1/(p-1) < 2/p$ so

$$\prod_p \left(1 + \frac{1}{p(p-1)}\right) < \prod_p \left(1 + \frac{2}{p^2}\right) < \prod_p e^{2/p^2} = e^{\sum_p 2/p^2} < e^{2C}$$

We can safely deduce that $\sum_p 1/p^2 < C$ because it is a convergent series, since the above is convergent by Theorem 1.2.2, $\sum_n 1/n$ with n only squarefull numbers is also convergent.

As for α so that $\sum_n 1/n^\alpha$ is also convergent, my first guess will be $\alpha > 1/2$, this is because with $\alpha = 1/2$ we will have $1/p$ term in the series and it will cause things to blow up. Another clue is in the fact that involving an exponent α means that the upper bound becomes

$$e^{\sum_p 2/p^{2\alpha}}$$

and if α goes below $\leq 1/2$ we will have an divergent series while $\sum_n 1/n^\beta$ is convergent if $\beta > 1$ by the integral test.

Exercise 1.3.1. **Page** 22. We want to show that

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

using L'Hospital's rule. From what I know L'Hospital's rule only works if the limit is indefinite like $0/0$ or ∞/∞ but looks like I was wrong, you can use is even if it's not indefinite.

So we need to do a derivative w.r.t x on the integral above, how do we do it? for now assume that the integral is indefinite

$$\int \frac{dt}{\log t} = F(t) \qquad \longrightarrow \qquad \int_2^x \frac{dt}{\log t} = F(x) - F(2)$$

Taking the derivative with respect to x means that

$$\frac{d}{dx} \int_2^x \frac{dt}{\log t} = \frac{d}{dx} F(x)$$

But in this case

$$\frac{d}{dx} F(x) = \frac{d}{dt} F(t)\Big|_{t=x} = \frac{d}{dt}\left(\int \frac{dt}{\log t}\right)\Big|_{t=x} = \frac{1}{\log x}$$

While (on the other hand)

$$\frac{d}{dx}\left(\frac{x}{\log x}\right) = \frac{\log x - 1}{\log^2 x} = \frac{1}{\log x} - \frac{1}{\log^2}$$

taking the ratio

$$\begin{aligned}\lim_{x\to\infty}\frac{x/\log x}{\int_2^x dt/\log t} &= \lim_{x\to\infty}\frac{1/\log x - 1/\log^2 x}{1/\log x}\\ &= \lim_{x\to\infty} 1-\frac{1}{\log x}\\ &= 1\end{aligned}$$

Page 24. Before Lemma 1.4.2. This is a bit confusing, well more than a bit actually :) "Another way of viewing this argument is that all but finitely many primes fall into the unique reduced residue class (mod 2); from this perspective, the correct generalization is in plain sight. Namely, take any integer q; then every prime $p \nmid q$ has to fall into one of the $\varphi(q)/q$ reduced residue classes (mod q), and this forces the proportion of primes to be at most $\varphi(q)/q$."

First, $\varphi(q)$ is the Euler totient function, *i.e.* the number of numbers $< q$ that are co-prime to q. The original logic was that since half of all integers are even, so the proportion of prime numbers can only be at most 1/2. So at first, this looks a lot like the logic of sieve. Since you know that 2 is prime any multiple of 2 cannot be prime and so half of the numbers are gone. But this is not what we are doing, we are not doing sieve.

Instead what happens is this, if we choose $q = 4$ instead of 2, now if we group the integers as follows

$$\{\boldsymbol{1}, 2, \boldsymbol{3}, 4\}, \{\boldsymbol{5}, 6, \boldsymbol{7}, 8\}, \{\boldsymbol{9}, 10, \boldsymbol{11}, 12\}, \ldots$$

i.e. we are grouping them as residue classes of (mod 4), we see that each ***bold*** number is co-prime to 4, now the number itself might bot be prime, *e.g.* $\boldsymbol{9}$, but ***they*** are all co-prime to 4. Recall that $\gcd(a, q) = \gcd(a + qm, q)$ so if $a \equiv b \pmod{q}$ then $\gcd(a, q) = \gcd(b, q)$ and so in each residue class the number of numbers that are co-prime to a stays the same.

A number can only be prime if it is co-prime to q, which in this case is 4, this is a necessary condition, not a sufficient one, but we are only interested in the upper bound here so the necessary condition is sufficient :)

So if we group the integers into the residue classes of q there will be $\varphi(q)$ numbers that are co-prime to q and so the upper bound of the ratio of the prime numbers to all of the numbers is obviously $\varphi(q)/q$. But of course there's a caveat, this is correct only for the

second residue class and beyond, in the first residue class, $\{\boldsymbol{1},\underline{2},\boldsymbol{3},4\}$, 2 is also prime but it doesn't contribute towards $\varphi(q)$ because $2|4$, but this doesn't matter since the upper bound of the total ratio is given by

$$\frac{(\Delta+\varphi(q))+\varphi(q)+\varphi(q)+\ldots}{q+q+q+\ldots}=\frac{\Delta+\infty\cdot\varphi(q)}{\infty\cdot q}=\frac{\varphi(q)}{q}$$

Now, the statement "all but finitely many primes fall into the unique reduced residue class (mod 2);" means this, say for our $q=4$ example above, each residue class, whether the first, second or third, each of them can only take a finite amount of prime numbers and each prime number must of course fall into only one of them, ergo the word "unique", that's what the statement above means.

Page 24. Top of page, "the partial products $\prod_{2\leq n\leq x} n/(n-1)$ telescope to $\lfloor x\rfloor$", it telescope because

$$\prod_{2\leq n\leq x}\frac{n}{n-1}=\frac{\cancel{2}}{1}\cdot\frac{\cancel{3}}{\cancel{2}}\cdot\frac{\cancel{4}}{\cancel{3}}\cdots\frac{x}{\cancel{x-1}}=\frac{x}{1}$$

Page 24. Lemma 1.4.2. The first equality, recall that due to its multiplicity $\varphi(q)=\prod_{p_i}p_i^{\alpha_i-1}(p_i-1)=\prod_{p_i}p_i^{\alpha_i}(1-1/p_i)$, so when you divide it by q, the $p_i^{\alpha_i}$ terms disappear and you're left with only the $\prod_{p_i}(1-1/p_i)$.

In physics I always use the expansion $\frac{1}{1-x}=1+x+x^2+\ldots$, *i.e.* the geometric series, here, we use this a lot too :) to get the inequality $\varphi(q_x)/q_x\leq(\log x)^{-1}$, we need to invert it

$$\frac{1}{\prod_{p\leq x}1/(1-1/p)}=\prod_{p\leq x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\ldots\right)=\sum_{n:p|n,p\leq x}\frac{1}{n}\geq\sum_{n\leq x}\frac{1}{n}\geq\log x$$

and then we invert it again and y doing so reverses the inequality sign as well.

Page 24. Last equation on page, we need to be careful here, first we choose our desired ϵ then to get $\varphi(q)/q<\epsilon/2$ we need to choose q, and finally once we've fixed q we can choose x big enough to get $\varphi(q)/x+\nu(q)/x<\epsilon/2$.

Page 25. Last sentence of first paragraph, "the second product below telescopes so is

easy to compute",

$$\begin{aligned}\prod_{n=2}^{\infty}\frac{n^2}{n^2-1} &= \frac{2^2}{2^2-1}\cdot\frac{3^2}{3^2-1}\cdot\frac{4^2}{4^2-1}\cdots \\ &= \frac{2\cancel{(3-1)}}{(2-1)\cancel{(2+1)}}\cdot\frac{\cancel{(2+1)}\cancel{(4-1)}}{\cancel{(3-1)}\cancel{(3+1)}}\cdot\frac{\cancel{(3+1)}\cancel{(5-1)}}{\cancel{(4-1)}\cancel{(4+1)}}\cdots \\ &= \frac{2}{1}\end{aligned}$$

only the first term survives.

Page 25. Eq (1.21), it's just a different way of writing

$$\int_{3/2}^{x}\frac{1}{t}\pi'(t)dt = \int_{3/2}^{x}\frac{1}{t}\frac{d\pi(t)}{\cancel{dt}}\cancel{dt} = \int_{3/2}^{x}\frac{1}{t}d\pi(t)$$

where the cancellation is basically the chain rule

Page 30, Eq (1.29) and Eq (1.30), these two might be confusing if we just look at what was done before them, to see it clearly let's first denote things as

$$\Psi(x,k) = \psi(x) - \psi(x/2) + \psi(x/3) - \cdots \pm \psi(x/k), \qquad \pm \text{ depending on whether } k \text{ is even or odd}$$

we now want to compare $\Psi(x,k)$ to $T(x) - 2T(x/2)$, this is what Eq (1.29) and (1.30) are about.

Say k is even, then we can group $T(x) - 2T(x/2)$ this way

$$\begin{aligned}T(x) - 2T(x/2) &= \psi(x) - \psi(x/2) + \psi(x/3) - \cdots - \psi(x/k) \\ &\quad +[\psi(x/k+1) - \psi(x/k+2)] + [\psi(x/k+3) - \psi(x/k+4)] + \ldots \\ &= \Psi(x,k) + [\psi(x/k+1) - \psi(x/k+2)] + [\psi(x/k+3) - \psi(x/k+4)] + \ldots\end{aligned}$$

the thing to note here is that each square bracket is ≥ 0 therefore $\Psi(x,k) \leq T(x) - 2T(x/2)$. If k is odd, we group it a slightly different way

$$\begin{aligned}T(x) - 2T(x/2) &= \psi(x) - \psi(x/2) + \psi(x/3) - \cdots + \psi(x/k) \\ &\quad -[\psi(x/k+1) - \psi(x/k+2)] - [\psi(x/k+3) - \psi(x/k+4)] - \ldots \\ &= \Psi(x,k) - [\psi(x/k+1) - \psi(x/k+2)] - [\psi(x/k+3) - \psi(x/k+4)] + \ldots\end{aligned}$$

again, each square bracket is ≥ 0 but there is now a minus sign in front of each of them so therefore for k odd we have $\Psi(x, k \geq T(x) - 2T(x/2))$ and finally, the reason we have

less/greater than or *equal* to sign is because some of those $\psi(x/m)$ can be zero since they are guaranteed zero if the argument is less than 2.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Exercise 1.3.2, **Page** 22, show that $p_n \sim n \log n$. The hint tells us that we need to show that if $a_n \sim b_n$ then $a_n \log a_n \sim b_n \log b_n$, let's do this first.

The key is to use L'Hospital's rule

$$\begin{aligned}\lim_{n\to\infty} \frac{a_n \log a_n}{b_n \log b_n} &= \lim_{n\to\infty} \frac{a_n}{b_n} \cdot \frac{\log a_n}{\log b_n} \\ &= \lim_{n\to\infty} 1 \cdot \frac{1/a_n}{1/b_n}, \qquad \lim_{n\to\infty} \frac{a_n}{b_n} = 1 \text{ by hypothesis} \\ &= 1\end{aligned}$$

We then set $a_n = p_n \log p_n$ and $b_n = n$, we now need to show that $p_n/\log p_n \sim n$

$$\begin{aligned}\lim_{n\to\infty} \frac{p_n \log p_n}{n} &= \lim_{n\to\infty} \frac{p_n \log p_n}{\pi(p_n)}, \qquad \pi(p_n) \sim p_n \log p_n \text{ from PNT} \\ &= \lim_{n\to\infty} \frac{p_n/\log p_n}{p_n/\log p_n} \\ &= 1\end{aligned}$$

Finally, as a consequence of the above result, *i.e.* $a_n \sim b_n \to a_n \log_n \sim b_n \log b_n$ we have

$$\begin{aligned}1 = \lim_{n\to\infty} \frac{p_n \log p_n \log(p_n \log p_n)}{n \log n} &= \lim_{n\to\infty} \frac{p_n}{n \log n} + \frac{\log p_n \log(p_n \log p_n)}{\pi(n) \log \pi(n)} \\ &= \lim_{n\to\infty} \frac{p_n}{n \log n} + \frac{\log^2 p_n + \log\log p_n}{p_n/\log p_n \log(p_n/\log p_n)} \\ &= \lim_{n\to\infty} \frac{p_n}{n \log n} + \frac{\log^2 p_n + \log\log p_n}{p_n - \log\log p_n/\log p_n} \\ &= \lim_{n\to\infty} \frac{p_n}{n \log n} + \frac{p_n}{p_n} \cdot \frac{\log^2 p_n/p_n + \log\log p_n/p_n}{1 - \log\log p_n/p_n \log p_n} \\ &= \lim_{n\to\infty} \frac{p_n}{n \log n} + 0 \\ 1 &= \lim_{n\to\infty} \frac{p_n}{n \log n}\end{aligned}$$

Exercise 1.4.3, **Page** 26, so we have non-negative function f (for $x > x_0$) and $f(x) \to \infty$ as $x \to \infty$, need to find a set of integers $\mathcal{A}$ where

$$\sum_{a\in\mathcal{A}} \frac{1}{a} = \infty \qquad\qquad \liminf_{x\to\infty} \frac{A(x)}{f(x)} = 0$$

We can follow the hint or just reuse (1.21), replacing $\pi(x)$ with $A(x)$ (the function that counts the members of $\mathcal{A}$ less than equal to x) and the lower integration limit to $N-1$ instead of $3/2$

$$\begin{aligned}\sum_{a\in\mathcal{A}}\frac{1}{a} &= \int_{N-1}^{x}\frac{dA(t)}{t}\\ &= \frac{A(x)}{x}-\frac{A(N-1)}{N-1}+\int_{N-1}^{x}\frac{A(t)}{t^2}dt\\ &= \int_{N-1}^{x}\frac{A(t)}{t^2}dt+O(1)\end{aligned}$$

Since we are not including every number we know that $A(x)$ is at most x so $A(x)/x$ is at most 1, ergo the $O(1)$.

But I actually don't understand this problem, say $f(x)=\log x$ which meets our criteria above, if $\liminf_{x\to\infty} A(x)/f(x)=0$, does it mean that $A(x)$ is slower than $\log(x)$? if that's the case the integral above will be finite and the sum $\sum 1/a$ will not be divergent which is a contradiction.

Recall that the definition of lim inf is

$$\liminf_{x\to\infty} g(x) = \lim_{n\to\infty}\left(\inf_{x>n} g(x)\right) = L$$

where inf means the lowest value in that set which in this case is the lowest value of $g(x)$ for $x>n$. Now the definition of $\lim_{n\to\infty}$ in itself means for every number $\varepsilon>0$ there is some number $M>0$ such that

$$\left|\left(\inf_{x>n} g(x)\right)-L\right|<\varepsilon \qquad \text{whenever} \qquad n>M$$

so here once ε is given we then choose an M such that $|(\inf_{x>M} g(x))-L|<\varepsilon$ (we have replaced $x>n\to x>M$ since $n>M$) and this must be true for every $x>n>M$. In our case $g(x)=A(x)/f(x)$ and $L=0$.

Note that $A(x)$ just like $\pi(x)$ is piecewise continuous. So what we need to do is to leave gaps in the set $\mathcal{A}$ so that say for some $x>M$ there is a section $x\in(M<a,b)$ where $A(x)$ stays constant meanwhile $f(x)$ is always growing, but this also means that since $A(x)$ has been stagnant for some time $A(x)/f(x)$ in $(a>m,b)$ can be set to be less than ε which can be achieved by extending the stagnation interval to inhibit the growth of $A(x)$, we need to do this periodically because ε can be any real number.

The only thing left is to see if producing gaps like this will still result in divergent $\sum 1/a$. I actually have a "counter example", say we start with the harmonic series $1/n$ and we pick only a few numbers every e^x, *i.e.*

$$\sum_{n=\lceil e^1\rceil+1}^{\lceil e^1\rceil+2} \frac{1}{n} + \sum_{n=\lceil e^2\rceil+1}^{\lceil e^2\rceil+2} \frac{1}{n} + \sum_{n=\lceil e^3\rceil+1}^{\lceil e^3\rceil+2} \frac{1}{n} + \dots$$

We can estimate this series by replacing each sum with an integral (of course the value of the integral will be $>$ than the corresponding sum) and the integrals will yield

$$\begin{aligned}\int_{e^1}^{e^1+3} \frac{dx}{x} + \int_{e^2}^{e^2+3} \frac{dx}{x} + \int_{e^3}^{e^3+3} \frac{dx}{x} + \dots &= \log\left(\frac{e^1+3}{e^1}\right) + \log\left(\frac{e^2+3}{e^2}\right) + \log\left(\frac{e^3+3}{e^3}\right) + \dots \\ &= \sum_{k=1}^{\infty} \log\left(\frac{e^k+3}{e^k}\right)\end{aligned}$$

If we do an integral test on the above we'll get $li_2\left(-3e^{-x}\right)$, the dilogarithm function and the limit as $x \to \infty$ is zero and so by the integral test it is convergent, so in this case we remove too many things. If instead of e^k we pick k^m

$$\sum_{k=1}^{\infty} \log\left(\frac{k^m+3}{k^m}\right)$$

the above is only divergent for $m = 1$ and is convergent for all $m > 1$.

Actually we don't need to go that far, say from the harmonic series we only pick up the following

$$\frac{1}{1} + \frac{1}{10} + \frac{1}{100} + \dots = \frac{1}{1-\frac{1}{10}} = \frac{10}{9}$$

then we have a convergence series. So we need to be careful as to not produce too large a gap, the problem is that as $x \to \infty$ the gaps need to be bigger and bigger.

A cautionary tale in taking a limit, during my adventure deploying the root test

$$\lim_{k\to\infty} |a_k|^{1/k} = \lim_{k\to\infty} \left(\log\left(\frac{k+3}{k}\right)\right)^{1/k}$$

for k really big $k + 3/k \to 1$ and $\log(k + 3/k) \to 0^+$, the k^{th} root of a number less than 1 is obviously less than 1, the bigger k is the closer to 1 the k^{th} root is, so at a glance it

seems like the limit is less than 1 but this is wrong. If we take the log we get

$$\begin{aligned}\lim_{k\to\infty} \log\left(\log\left(\frac{k+3}{k}\right)\right)^{1/k} &= \lim_{k\to\infty} \frac{\log\left(\log\left(\frac{k+3}{k}\right)\right)}{k} \\ &= 0 \\ \to \lim_{k\to\infty} \left(\log\left(\frac{k+3}{k}\right)\right)^{1/k} &= 1\end{aligned}$$

This is the same situation as $\lim_{x\to\infty} 1/x$, $1/x$ is never zero no matter what x is but the limit $1/x$ is still 0.

Note that

$$\liminf_{x\to\infty} \frac{A(x)}{f(x)} = 0 \qquad \text{means that} \qquad A(x) \ll f(x) \quad \text{i.e} \quad A(x) = O(f(x))$$

while what we want is the reverse $f(x) = O(A(x))$

Another thing is that $A(x)$ is monotonically increasing as it is just counting the number of integers in $\mathcal{A}$ so say $f(x) = \log\log\log x$ then $A(x)$ has to be slower than $\log\log\log$ for the $\liminf$ to be zero, but if $A(x)$ is this slow it will not diverge ¯\(°_o)/¯