3.2 The Sieve of Eratosthenes

Note Title 12/9/2004

1. Test all primes $p \le \sqrt{701}$ to see if 701 is prime.

$\sqrt{701} = 26.5$ $\therefore$ test 2, 3, 5, 7, 11, 13, 17, 19, 23
All do not divide 701. $\therefore$ 701 is prime
$\sqrt{1009} = 31.7$, 1009 not divisible by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

2.

101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

$14 < \sqrt{200} < 15$, $\therefore$ stop at $p = 13$

3. If $p \nmid n$ for all primes $p < \sqrt[3]{n}$, $n > 1$, Then n is either prime or the product of two primes

Pf: Assume n is composite, and let
$n = p_1 p_2 \cdots p_r$, and assume $r \ge 3$

Note: p_i not among primes $p < \sqrt[3]{n}$. $\therefore p_1 \geq \sqrt[3]{n}$,
$p_2 > p_1 \geq \sqrt[3]{n}$.

We know that $1 < \sqrt[3]{n} < p_i \leq \sqrt{n}$

$\therefore \sqrt[3]{n} \leq p_1 \leq \sqrt{n}$

$\sqrt[3]{n} < p_2 \leq \sqrt{n}$

$\sqrt[3]{n} < p_3 < \sqrt{n}$

$\therefore n = (\sqrt[3]{n})(\sqrt[3]{n})(\sqrt[3]{n}) < p_1 p_2 p_3 = n$,
or $n < n$. $\therefore$ $r < 3$, or $r = 2$ or $r = 1$.

$\therefore$ n is either prime $(r=1)$ or
is the product of two primes $(r=2)$.

4. (a) $\sqrt{p}$ is irrational for any prime p.

Pf: Assume $\sqrt{p} = \frac{r}{s}$, some integers r, s.

Let $d = \gcd(r, s)$. Let $r_p = \frac{r}{d}$, $s_p = \frac{s}{d}$

$\therefore \gcd(r_p, s_p) = 1$, by Corollary 1, p. 23

Also $\frac{r}{s} = \frac{r_p}{s_p}$. $\therefore \sqrt{p} = \frac{r_p}{s_p}$

$\therefore p = \frac{r_p^2}{s_p^2}$, $p s_p^2 = r_p^2$. $\therefore p \mid r_p^2 \Rightarrow p \mid r_p$

$\therefore$ Let $r_p = px$. $\therefore r_p^2 = p^2 x^2 = p s_p^2$, or

$p x^2 = s_p^2$. $\therefore p \mid s_p$. $\therefore \gcd(r_p, s_p) \neq 1$

$\therefore$ There doesn't exist integers r, s s.t. $\sqrt{p} = \frac{r}{s}$

(b) $a > 0$, $\sqrt[n]{a}$ rational, then $\sqrt[n]{a}$ is an integer.

Pf: Let $\sqrt[n]{a} = \frac{r}{s}$, r, s integers, s.t. $\gcd(r,s) = 1$.

Let $r = p_1 \cdots p_x$, $s = q_1 \cdots q_y$

$\therefore p_i \neq q_j$

$\therefore (q_1^n \cdots q_y^n) a = p_1^n \cdots p_x^n$

$\therefore p_1^n \cdots p_x^n \mid a$. $\therefore$ Let $a = (p_1^n \cdots p_x^n) z$

$\therefore (q_1^n \cdots q_y^n)(p_1^n \cdots p_x^n) z = p_1^n \cdots p_x^n$

$\therefore (q_1^n \cdots q_y^n) z = 1$. $\therefore q_j = 1$ for all j.

$\therefore s = 1$, $\therefore \frac{r}{s}$ is an integer.

(c) For $n \geq 2$, $\sqrt[n]{n}$ is irrational.

Pf: Suppose $\sqrt[n]{n}$ is rational. From (b), it is an integer. Let $\sqrt[n]{n} = a$.

$\therefore n = a^n$. But $n < 2^n$.

$\therefore a^n < 2^n$, so $a < 2$, or $a = 1$.
$\therefore n = 1^n = 1$, a contradiction.

5. Any composite 3-digit number must have a prime factor ≤ 31.

Pf: 999 is largest 3-digit number.
$\sqrt{999} = 31.6\ldots$ 31 is prime, so if a is composite, largest prime divisor is $\leq \sqrt{a}$, so 31 is largest possible prime divisor.

6. Number of primes is infinite.

Pf: Assume only finite number: $p_1, p_2, \ldots p_n$
Let A be the product of any r of these,
so $A = p_{a_1} p_{a_2} \cdots p_{a_r}$, $a_i \in \{1, 2, \ldots n\}$

Consider $B = p_1 p_2 \cdots p_n / A$

$$= \frac{p_1 p_2 \cdots p_n}{p_{a_1} p_{a_2} \cdots p_{a_r}} = p_{b_1} p_{b_2} \cdots p_{b_s}$$

where $a_i \neq b_j$ (i.e., factoring out p_{a_i}), so
$\{p_{a_i}\} \cap \{p_{b_j}\} = \emptyset$, and $\{p_{a_i}\} \cup \{p_{b_j}\} = \{p_1, p_2 \ldots, p_n\}$

So, A and B have no common factors.

Then each p_k of $p_1, p_2, \dots, p_n$ divides either A or B, but not both.

Since $A > 1$, $B > 1$, Then $A+B > 1$.
$A+B$ must have a prime factor, p,
and $p \mid (A+B)$ is an integer, and
$p \in \{p_1, p_2, \dots, p_n\}$ since assuming finite primes

Suppose $p \mid A$. $\therefore$ $px = A+B$, some x,
and $py = A$, some y.
$\therefore$ $px = py + B$, $\therefore$ $p(x-y) = B$, so $p \mid B$,
a contradiction.

7. Prove infinitely many primes using $N = p! + 1$

Pf: Assume finitely many primes, p_n the largest.
Consider $N = p_n! + 1$

$\therefore$ $N = 1 \cdot 2 \cdots p_n + 1$.

N must have a prime divisor p_k, $1 \le k \le n$.
since assuming finite # primes.

And $p_K \mid 1 \cdot 2 \cdot 3 \cdots p_n$ since p_K is one of

The members of $p_n!$.

$\therefore p_K \mid (N - p_1 p_2 \cdots p_n)$. $\therefore p_K \mid 1$, $p_K = 1$,

a contradiction.

8. Prove infinitude of primes using

$$N = p_2 \cdots p_n + p_1 p_3 \cdots p_n + \dots + p_1 p_2 \cdots p_{n-1}$$

Pf: Assume finite # of primes $p_1, p_2, \dots p_n$

Consider $q_K = p_1 p_2 \cdots p_n$, s.t. each term $p_i \neq q_K$.

$\therefore q_1 = p_2 p_3 \cdots p_n$

$q_2 = p_1 p_3 p_4 \cdots p_n$

$\vdots$

$q_n = p_1 p_2 p_3 \cdots p_{n-1}$

$\therefore p_K \nmid q_K$

Let $N = q_1 + q_2 + \cdots q_n = \sum_{i=1}^{n} q_i$

N must have a prime divisor from $p_1, \ldots, p_n$
Let p_k $(1 \le k \le n)$ be that prime divisor.

But since $p_k \mid N$ and $p_k \mid q_i$, $i \ne k$,

Then $p_k \mid \left(N - \sum_{i=1, i\ne k}^{n} q_i\right)$

But then $N - \sum_{i=1, i \ne k}^{n} q_i = q_k$

$\therefore$ $p_k \mid q_k$, a contradiction.

9. (a) if $n > 2$, Then $\exists p$ s.t. $n < p < n!$

Pf: For $n > 2$, clearly $2n < n! = 1 \cdot 2 \cdot \ldots \cdot n$
From Bertrand's conjecture, $\exists$ a prime p
S.t. $n < p < 2n$ $\therefore$ $n < p < 2n < n!$

Pf: (using author's hint)

For $n > 3$, $n < n! - 1 < n!$
If $n! - 1$ is prime, we're done
If $n! - 1$ is not prime, let p be a prime divisor. $\therefore$ $p < n! - 1$

Assume $p \le n$. Then p is one of

The terms of $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$, so $p | n!$

$\therefore p | n!$ and $p | (n!-1)$

$\therefore p | n! - (n!-1) = 1$

$\therefore p > n$. $\therefore n < p < n!-1 < n!$

(b). For $n > 1$, every prime divisor of $n!+1$ is an odd integer $> n$

Pf: First, $n!+1$ is odd, since $n!$ is even, as it contains 2, and $2x$ is even for all x.

$\therefore$ 2 will never divide $n!+1$, so every prime divisor of $n!+1$ is odd.

Now suppose every prime divisor p_i of $n!+1$ is s.t. $p_i \le n$.

Let $P = n!+1$

Clearly, $p_i | n!$, since p_i is one of the members of $n!$

Since $p_i | P$, then $p_i | (P - n!)$, and

$P - n! = 1$. $\therefore p_i | 1$, a contradiction

$\therefore p_i > n$

10. Let q_n be smallest prime s.t. $q_n > P = p_1 p_2 \cdots p_n + 1$
Show $q_n - (p_1 p_2 \cdots p_n)$ is prime for $n = 1, 2, \ldots, 5$

$q_1: \; 2+1 = 3 \quad \therefore \; q_1 = 5$
$q_2: \; 2 \cdot 3 + 1 = 7 \qquad q_2 = 11$
$q_3: \; 2 \cdot 3 \cdot 5 + 1 = 31 \qquad q_3 = 37$

$q_4: \; 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \qquad q_4 = 223$

$q_5: \; 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \qquad q_5 = 2333$

$\therefore \; q_1 - (p_1) = 5 - 2 = 3$
$q_2 - (p_1 p_2) = 11 - 6 = 5$
$q_3 - (p_1 p_2 p_3) = 37 - 30 = 7$

$q_4 - (p_1 p_2 p_3 p_4) = 223 - 210 = 13$

$q_5 - (p_1 p_2 p_3 p_4 p_5) = 2333 - 2310 = 23$

11. Let $d_n = p_{n+1} - p_n$. Find five solutions to $d_n = d_{n+1}$

$d_1 = p_2 - p_1 = 3 - 2 = 1$
$d_2 = p_3 - p_2 = 5 - 3 = 2$
$d_3 = p_4 - p_3 = 7 - 5 = 2 \qquad \therefore \; d_2 = d_3$
$d_4 = p_5 - p_4 = 11 - 7 = 4$

$$d_5 = p_6 - p_5 = 13 - 11 = 2$$

$$d_6 = p_7 - p_6 = 17 - 13 = 4$$

$$d_7 = p_8 - p_7 = 19 - 17 = 2$$

$$d_8 = p_9 - p_8 = 23 - 19 = 4$$

$$d_9 = 29 - 23 = 6$$

$$d_{10} = 31 - 29 = 2$$

$$d_{11} = 37 - 31 = 6$$

$$d_{12} = 41 - 37 = 4$$

$$d_{13} = 43 - 41 = 2$$

$$d_{14} = 47 - 43 = 4$$

$$d_{15} = 53 - 47 = 6$$

$$d_{16} = 59 - 53 = 6 \quad \therefore d_{15} = d_{16}$$

$$61 - 59 = 2$$

$$67 - 61 = 6$$

$$\vdots$$

$$157 - 151 = 6$$

$$163 - 157 = 6 \quad \therefore d_{36} = d_{37}$$

$$\vdots$$

$$173 - 167 = 6$$

$$179 - 173 = 6 \quad \therefore d_{40} = d_{39}$$

$$\vdots$$

$$211 - 199 = 12$$

$$223 - 211 = 12 \quad \therefore d_{47} = d_{46}$$

12. Let p_n be n-th prime number. Prove:

(a) $p_n > 2n-1$, for $n \geq 5$

Pf: For $n=5$, $p_n = 11 > 2(5)-1 = 9$

Assume true for K: $p_K > 2K-1$

$\therefore p_K + 2 > (2K-1) + 2 = 2(K+1) - 1$

Since $p_K + 1$ is even, then next possible prime is $p_K + 2$.

$\therefore p_{K+1} \geq p_K + 2$

$\therefore p_{K+1} > p_K + 2 > 2(K+1) - 1$, so if assertion true for K, then it's true for $K+1$.

$\therefore$ True for all $n \geq 5$

(b) None of $P_n = p_1 p_2 \cdots p_n + 1$ is a perfect square.

Pf: First note that since $p_1 = 2$, then $p_1 p_2 \cdots p_n$ is even, so $p_1 p_2 \cdots p_n + 1$ is odd.

By Division Algorithm, $P_n = 4k + r$, $r = 0, 1, 2, 3$
But since P_n is odd, $r = 1, 3$
If $r = 1$, then $p_1 p_2 \cdots p_n + 1 = 4k + 1$, so

$$p_1 p_2 \cdots p_n = 4k, \text{ so } p_2 p_3 \cdots p_n = 2k$$

But $p_2 \cdots p_n$ is odd since all factors are odd, and $2k$ is even.
$\therefore r \neq 1$.

$\therefore P_n = 4k + 3$ for all n.

Suppose $P_n = s^2$, some s, and $s^2 = 4k + 3$

Since s^2 is odd, so is s.
$\therefore s = 2a + 1$, some a.

$\therefore s^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 4k + 3$
$\therefore 4a^2 + 4a = 4k + 2$
$2a^2 + 2a = 2k + 1$
But $2a^2 + 2a$ is even, and $2k+1$ is odd.

$\therefore$ There is no s s.t. $P_n = s^2$

(c) $\frac{1}{p_1} + \frac{1}{p_2} + \cdots \frac{1}{p_n}$ is never an integer.

Pf: Let $P = p_1 p_2 \cdots p_n$, and suppose

$\frac{1}{p_1} + \frac{1}{p_2} + \cdots \frac{1}{p_n} = a$, some integer a.

$$\therefore \frac{P}{p_1} + \frac{P}{p_2} + \cdots \frac{P}{p_n} = aP$$

For p_1, $p_1 \mid aP$ and $p_1 \mid \frac{P}{p_2}$, $p_1 \mid \frac{P}{p_3}, \ldots p_1 \mid \frac{P}{p_n}$

$$\therefore p_1 \mid (P - p_2 - p_3 - \cdots - p_n)$$

$\therefore p_1 \mid \frac{P}{p_1} \Rightarrow p_1 \mid p_2 p_3 \cdots p_n$, a contradiction.

Similar reasoning applies for $p_2, \ldots, p_n$

$\therefore$ No such integer $a = \frac{1}{p_1} + \cdots + \frac{1}{p_n}$ exists.

13. (a) If $n \mid m$, then $R_n \mid R_m$

Pf: First prove Lemma:

if $m = kn$, then

$$x^m - 1 = (x^n - 1)(x^{(k-1)n} + x^{(k-2)n} + \cdots + x^n + 1)$$

Pf: From problem #3, p. 7, we know that

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \dots + a + 1)$$

$\therefore$ let $a = x^n$

$$\therefore x^{kn} - 1 = (x^n - 1)(x^{n(k-1)} + x^{n(k-2)} + \dots + x^n + 1)$$

Since $kn = m$,

$$\therefore x^m - 1 = (x^{n(k-1)} + x^{n(k-2)} + \dots + x^n + 1)$$

Now $R_n = \dfrac{(10^n - 1)}{9}$, $R_m = \dfrac{(10^m - 1)}{9}$

$$\therefore \frac{R_m}{R_n} = \frac{10^m - 1}{10^n - 1} = \frac{10^{kn} - 1}{10^n - 1}$$

By the Lemma, $10^{kn} - 1 = (10^n - 1)(10^{n(k-1)} + \dots + 10^n + 1)$

$$\therefore \frac{R_m}{R_n} = \frac{(10^n - 1)(10^{n(k-1)} + \dots + 10^n + 1)}{10^n - 1}$$

$$= (10^{n(k-1)} + \dots + 10^n + 1)$$

$\therefore n \mid m \Rightarrow R_n \mid R_m$

(6) if $d \mid R_n$ and $d \mid R_m$, Then $d \mid R_{n+m}$

Pf: $R_n = \dfrac{10^n - 1}{9}$, $R_m = \dfrac{10^m - 1}{9}$

$$R_{n+m} = \frac{10^{n+m} - 1}{9} = \frac{10^n 10^m - 1}{9}$$

$$= \frac{10^n 10^m - 10^m + 10^m - 1}{9}$$

$$= \frac{10^m (10^n - 1) + 10^m - 1}{9}$$

$$= 10^m R_n + R_m$$

$\therefore d \mid R_n \Rightarrow R_n = dr$, some r

$d \mid R_m \Rightarrow R_m = ds$, some s

$\therefore R_{n+m} = 10^m R_n + R_m$
$= 10^m dr + ds = d(10^m r + s)$

$\therefore d \mid R_{n+m}$

(c) if $\gcd(n,m)=1$, then $\gcd(R_n, R_m)=1$

Pf: $\gcd(n,m)=1 \Rightarrow 1 = an + bm$, some a, b.

Let $d = \gcd(R_n, R_m)$. $\therefore d \mid R_n, d \mid R_m$

Since $n \mid an$, then $R_n \mid R_{an}$ by (a)
Since $m \mid bm$, then $R_m \mid R_{bm}$ by (a)

Since $d \mid R_n$ and $R_n \mid R_{an}$, then $d \mid R_{an}$

Since $d \mid R_m$ and $R_m \mid R_{bm}$, then $d \mid R_{bm}$

$\therefore$ by (b) $d \mid R_{an+bm}$

But $R_{an+bm} = R_1 = 1$. $\therefore d \mid 1$, $\therefore d=1$

14. Find prime factors of R_{10}

Since $2 \mid 10$ and $5 \mid 10$, then by 13(a), $R_2 \mid R_{10}$ and $R_5 \mid R_{10}$. $R_2 = 11$, $R_5 = 41 \cdot 271$.

$\therefore 11 \cdot 41 \cdot 271 \mid R_{10}$. But $\frac{R_{10}}{11 \cdot 41 \cdot 271} = 9091$, a prime

$\therefore R_{10} = 11 \cdot 41 \cdot 271 \cdot 9091$