3.1 The Fundamental Theorem of Arithmetic

Note Title 11/24/2004

1. n^2-2; $n=2 \Rightarrow 2^2-2 = 2$ All primes
$n=3 \Rightarrow 9-2=7$
$n=5 = 25-2 = 23$
$n=7 = 49-2 = 47$
$n=9 = 81-2 = 79$

2. $25 \stackrel{?}{=} p + a^2$. $a=1$ $p=24$ $\therefore$ No prime p for all possible values of a.
$a=2$ $p=21$
$a=3$ $p=16$
$a=4$ $p=9$
$a=5$ $p=0$

3. (a) If $3n+1$ is prime, so is $6m+1$

Pf: $3n+1$ prime $\Rightarrow 3n+1$ is odd. Let $p=3n+1$. Then $p-1=3n$ is even.
$\therefore$ n is even, $\therefore$ $n=2m$, some m,
$\therefore$ $p = 3(2m)+1 = 6m+1$

(b) Every integer of form $3n+2$ has a prime factor of that form.

Pf: Let p be any prime factor of $3n+2$
$\therefore$ $p = 3k+1$ or $3k+2$, some k, by Division Alg.

$\therefore 3n+2 = (3k_1+1)(3k_2+1)\cdots(3k_r+1)$, by Fund. Th. of Arith.

But this latter product is of form $[3^r k_1 \cdots k_r + \ldots + 1]$, where every term, except 1, is a factor of 3. $\therefore$ Product is of form $3q+1$, a contradiction.

(c) The only prime of form n^3-1 is 7.

Pf: $n^3-1 = (n-1)(n^2+n+1)$

For n^3-1 to be prime, $n>1$

For $n=2$, $n^3-1 = (2-1)(7) = 7$

For any $n>2$, $p = n^3-1$ will be a factor of two integers, neither of which is 1. $\therefore$ for $n \neq 2$, p can't be prime.

(d) The only prime p for which $3p+1$ is a perfect square is $p=5$.

Pf: $3(5)+1 = 16 = 4^2$

Suppose $3p+1 = n^2$, some $n \neq 4$

$\therefore 3p = n^2-1 = (n+1)(n-1)$

If $n+1=p$, Then $n-1=3$, $n=4$
Assume $n+1 \neq p$. $\therefore \gcd(n+1,p)=1$.
$\therefore n+1 \mid 3$, by Euclid's Lemma.
$\therefore n+1=1$ or 3, $\therefore n=2$. $\therefore 3p+1=4$,
$p=1$, a contradiction.
$\therefore n+1$ must be p, and $\therefore n$ must be 4

Similar reasoning for $n-1$.
If $n-1=p$, Then $n+1=3$, $n=2$, leading to contradiction of $3p+1=4$, $p=1$.
$\therefore n-1 \neq p$, Then $\gcd(n-1,p)=1$, $\therefore$
$n-1 \mid 3$ by Euclid's Lemma. $\therefore n-1=1$ or 3.
$\therefore n=4$.

(e) The only prime of form n^2-4 is 5.

Pf: Let $p = n^2-4 = (n+2)(n-2)$
Since p is prime, one of The factors must be 1 and The other must be p.

Suppose $n+2=p$, $\therefore n-2=1$, $\therefore n=3$,
$\therefore p=5$
Suppose $n+2=1$. $\therefore n=-1$, and
$\therefore p=n-2=-3$. $\therefore n+2 \neq 1$.
$\therefore$ Only possibility is $n=3$, $\therefore p=5$

4. $p \geq 5$, Then p^2+2 is composite

Pf: By Div. Alg., $p = 6k + r$, $0 \leq r < 6$

$r \neq 0$ as $p = 6k \Rightarrow 6 | p$
$r \neq 2$ as $p = 6k+2 \Rightarrow 2 | p$
$r \neq 3$ as $p = 6k+3 \Rightarrow 3 | p$
$r \neq 4$ as $p = 6k+4 \Rightarrow 2 | p$

$\therefore$ $p = 6k+1$ or $p = 6k+5$

$\therefore$ $p^2+2 = 36k^2 + 12k + 3$ or
$p^2+2 = 36k^2 + 60k + 27$

In either case, $3 | p^2+2$, so
p^2+2 is composite.

5. (a) p prime, $p | a^n \Rightarrow p^n | a^n$

Pf: By Corollary 1 (p. 41), $p | a^n \Rightarrow p | a$
$\therefore$ $a = pk$, some k, so $a^n = p^n k^n \Rightarrow p^n | a^n$

(b) If $\gcd(a,b) = p$, Then by (a) above, $p^2 | a^2$, $p^2 | b^2$,
so $\gcd(a^2, b^2) = p^2$

$\gcd(a^2, b) = p$

$\gcd(a^3, b^2) = p^2$

6. (a) For all $n > 1$, $n^4 + 4$ is composite

Pf: $n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$

Since $n > 1$, $n \geq 2$, $n^2 \geq 2n$, and

$\therefore n^2 - 2n \geq 0$, $n^2 - 2n + 2 \geq 2 > 0$

$\therefore$ Both factors are positive.

Since $n^4 + 4$ has two integer positive factors, it is composite.

Find the factors by guessing the roots (or using a calculator).

Note that $(1+i)(1+i) = 2i$, $(2i)^2 = -4$

$\therefore 1+i$ is a root, and $\therefore$ so is $1-i$

$\therefore (n-1-i)(n-1+i) = (n-1)^2 - i^2$

$= n^2 - 2n + 1 + 1$

$= n^2 - 2n + 2$,

and so $n^2 - 2n + 2$ is a factor

Find the other by division.

(b) If $n > 4$ is composite, then n divides $(n-1)!$

Pf: Since n is composite, let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the unique prime factorization.

If $r > 1$, then $n > p_i^{k_i}$, so $n-1 \geq p_i^{k_i}$
$\therefore$ since all integers $\leq n-1$ are terms of $(n-1)!$, then each $p_i^{k_i}$ is represented by one of the terms of $(n-1)!$. $\therefore p_1^{k_1} \cdots p_r^{k_r} \mid (n-1)!$

Suppose $r = 1$, so $n = p^k$. $k > 1$ since n is composite.
$\therefore n = p^{k-1} p$
$\therefore n > p$ and $n > p^{k-1}$
$\therefore n-1 \geq p$ and $n-1 \geq p^{k-1}$

If $p \neq p^{k-1}$, then each is represented in $(n-1)!$, so $p \cdot p^{k-1} = n \mid (n-1)!$

Suppose $p = p^{k-1}$, so $k = 2$. $\therefore n = p^2$
$\therefore n > p$, so $n-1 \geq p$
Since $n \geq 6$, then $p \neq 2$
And $2(n-1) < (n-1)!$ for $n > 4$
$\therefore 2(n-1)$ is a term of $(n-1)!$
$\therefore$ Each of p and $2p$ are terms of $(n-1)!$ $\therefore 2p^2 \mid (n-1)!$, so $p^2 \mid (n-1)!$ $\therefore p^2 = n \mid (n-1)!$

(c) $8^n + 1$, $n \geq 1$, is composite

Pf: $a^3 + 1 = (a+1)(a^2 - a + 1)$

$\therefore (2^n)^3 + 1 = (2^n + 1)(2^{2n} - 2^n + 1)$

$\therefore 2^n + 1 \mid 2^{3n} + 1$,

and $2^{3n} = 8^n$

$\therefore 2^n + 1 \mid 8^n + 1$

(d) $n > 11$, Then n is The sum of two composite numbers

Pf: Suppose n is even. Then $\exists K$ s.t. $n = 2K$.

$n = 2K = 6 + 2(K-3)$

$\therefore$ n is The sum of 6 ($= 2 \cdot 3$) and $2(K-3)$

If $K \geq 5$ (so $K-3 > 1$, so $2(K-3)$ is product of two numbers > 1), Then $2K \geq 10$, $n > 11$, and n is The sum of two composites.

Suppose n is odd. Then $\exists K$ s.t. $n = 2K+1$

$\therefore n = 2K+1$

$= 2(K-1) + 3$ 3 is prime

$= 2(K-2) + 5$ 5 is prime

$= 2(K-3) + 7$ 7 is prime

$= 2(K-4) + 9$

So, if $K \geq 6$, Then $2(K-4)$ is The

product of two numbers > 1, so $n = 2k+1 \geq 13$, and n is the sum of two composites.

7. Find all primes that divide $50!$

All primes < 50 will divide $50!$ since each is a term of $50!$
By Fund. Th. of Arithmetic, each term k of $50!$ that is non-prime has a unique prime factorization, and each term of the unique factorization of k is smaller than k, and so is a prime that is < 50. $\therefore$ There is no prime > 50 represented in this factorization of k.
$\therefore$ All primes < 50 are all the primes that divide $50!$

8. $p \geq q \geq 5$, p, q primes, $24 \mid p^2 - q^2$

Pf: From #4 above, $p = 6r+1$ or $6r+5$
$q = 6s+1$ or $6s+5$

Three possibilities

(1) $p = 6r+1$, $q = 6s+1$

(2) $p = 6r+5$, $q = 6s+5$

(3) $p = 6r+1$, $q = 6s+5$

The situation of $p = 6r+5$, $q = 6s+1$ is equivalent to #(3).

(1) Let $p = 6r+1$, $q = 6s+1$ $(r, s > 0,\ p, q \geq 7)$

Since $p, q \geq 5$, then $r, s \neq 0$

$\therefore p^2 - q^2 = (p+q)(p-q)$

$= (6r+1+6s+1)(6r+1-[6s+1])$

$= (6r+6s+2)(6r-6s)$

$= 2\cdot 6(3r+3s+1)(r-s)$

if r, s are both even or both odd, then $r-s$ is even and $\neq 0$, so $r-s = 2k$

$\therefore p^2 - q^2 = 2\cdot 6\cdot 2(3r+3s+1)(k)$

$= 24(3r+3s+1)(k)$. $\therefore 24 \mid p^2 - q^2$

if one is even and one is odd, then $3r+3s+1$ is even, so $3r+3s+1 = 2k$

$\therefore p^2 - q^2 = 2\cdot 6\cdot 2(k)(r-s) = 24(k)(r-s)$

$\therefore 24 \mid p^2 - q^2$

(2) Let $p = 6r+5$, $q = 6s+5$ $(r, s \geq 0,$ so $p, q \geq 5)$

$\therefore p^2 - q^2 = (p+q)(p-q)$

$(6r+5+6s+5)(6r-6s)$

$= (6r+5+6s+10)(6r-6s)$

$= 2\cdot 6(3r+3s+5)(r-s)$

if r, s are both even or both odd, then
$r-s$ is even and $\neq 0$, so $r-s = 2k$
$\therefore p^2-q^2 = 2\cdot 6\cdot 2\,(3r+3s+5)(k)$
$= 24\,(3r+3s+5)(k) \quad \therefore 24 \mid p^2-q^2$
if one is even, one odd, then
$3r+3s+5$ is even, so $3r+3s+5 = 2k$
$\therefore p^2-q^2 = 2\cdot 6\cdot 2\,(k)(r-s) = 24\,(k)(r-s)$
$\therefore 24 \mid p^2-q^2$

(3) $p = 6r+1,\ q = 6s+5 \quad (r>0,\ s\geq 0,\ \text{so } p, q \geq 5)$

$\therefore p^2-q^2 = (p+q)(p-q)$
$= (6r+1+6s+5)(6r-6s-4)$
$= (6r+6s+6)(6r-6s-4)$
$= 6\cdot 2\,(r+s+1)(3r-3s-2)$
If one is even, one odd, then $r+s+1$ is even,
so $r+s+1 = 2k$.
$\therefore p^2-q^2 = 24(k)(3r-3s-2)$, so $24 \mid p^2-q^2$
if both even or both odd, then
$3r-3s-2$ is even, so $3r-3s-2 = 2k$
$\therefore p^2-q^2 = 24(r+s+1)(k)$, so $24 \mid p^2-q^2$

9. (a). $2^4+1 = 17$
$2^8+1 = 257$
(b) $1^2+1 = 2 \qquad 4^2+1 = 17 \qquad 10^2+1 = 101$
$2^2+1 = 5 \qquad 6^2+1 = 37$

10. $p \neq 5,\ p \neq 2$, prove $10 \mid p^2-1$ or $10 \mid p^2+1$

Pf: p is of the form: $10K+1,\ 10K+3,\ 10K+7,\ 10K+9$.

$10K+\text{even}$: can factor out 2, so not prime.

$$(10K+1)^2 = 100K^2+20K+1 \quad \therefore 10 \mid p^2-1$$
$$(10K+3)^2 = 100K^2+60K+9 \quad \therefore 10 \mid p^2+1$$
$$(10K+7)^2 = 100K^2+140K+49 \quad \therefore 10 \mid p^2+1$$
$$(10K+9)^2 = 100K^2+180K+81 \quad \therefore 10 \mid p^2-1$$

11. (a) $2^3-1 = 7 \qquad 2^7-1 = 127$

$2^5-1 = 31 \qquad 2^{13}-1 = 8091$

(b) if $p = 2^k-1$ is prime, show k is odd if $k>2$

Pf: $a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\dots+ab^{n-2}+b^{n-1})$

$\therefore 4^n-1 = (4-1)(4^{n-1}+\dots+1)$

$= 3(4^{n-1}+\dots+1)$

$\therefore 3 \mid 4^n-1 \Rightarrow 3 \mid 2^{2n}-1 \quad (n \geq 1)$

$2n$ is even, so if $p = 2^k-1$ is prime, k must be odd ($n \geq 1 \Rightarrow 2n \geq 2$, so $k \geq 3$).

12. $1234 = 2 \cdot 617$

$10140 = 10 \cdot 1014 = 2 \cdot 5 \cdot 2 \cdot 507 = 2^2 \cdot 5 \cdot 3 \cdot 13^2$

$= 2^2 \cdot 3 \cdot 5 \cdot 13^2$

$36000 = 36 \cdot 1000 = 2^2 \cdot 3^2 \cdot 10 \cdot 25 \cdot 4$
$= 2^2 \cdot 3^2 \cdot 2 \cdot 5^3 \cdot 2^2$
$= 2^5 \cdot 3^2 \cdot 5^3$

13. If $n > 1$ not of form $6k+3$, Then $n^2 + 2^n$ is composite.

Pf: n of form $6k$, $6k+1$, $6k+2$, $6k+4$, $6k+5$

$6k$: $n^2 + 2^n = 36k^2 + 2^{6k}$. Since $k > 0$,
$2 \mid 36k^2 + 2^{6k}$ $\therefore$ composite

$6k+1$: $n^2 + 2^n = (6k+1)^2 + 2^{6k+1}$
$36k^2 + 12k + 1 + 2^{6k+1}$
$= 36k^2 + 12k + 1^{6k+1} + 2^{6k+1}$

From $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$
substitute $(-1 \cdot b)$ for b and get,
$a^n - (-1)^n b^n = (a+b)(a^{n-1} - a^{n-2}b + \dots + (-1)^{n-1} b^{n-1})$
$\therefore a^{6k+1} - (-1)^{6k+1} b^{6k+1} = a^{6k+1} + b^{6k+1} = (a+b)(\quad)$

$\therefore n^2 + 2^n = 36k^2 + 12k + 2^{6k+1} + 1$
$= 36k^2 + 12k + (2+1)(2^{6k} - \dots + (-1)^{6k} 1^{6k})$
$= 36k^2 + 12k + 3(2^{6k} - \dots + 1)$
$\therefore 3 \mid n^2 + 2^n$

$6k+2$: $n^2 + 2^n = (6k+2)^2 + 2^{6k+2}$
$= 36k^2 + 24k + 4 + 2^2 \cdot 2^{6k}$

$\therefore 2 \mid n^2+2^n$

$6K+4: \; n^2+2^n = 36K^2+48K+16+2^{6K+4}$

$\therefore 2 \mid n^2+2^n$

$6K+5: \; n^2+2^n = 36K^2+60K+25+2^{6K+5}$

$= 36K^2+60K+24+2^{6K+5}+1$

$= 36K^2+60K+24+(2+1)(2^{6K+4} \cdots)$

$= 3[\quad]$ similar to $6k+1$ above

$\therefore 3 \mid n^2+2^n$

Note for, $6K+3$, $36k^2+36K+9$, $9=8+1$, so can't use the $a^n+b^n=(a+b)(\quad)$ trick.

14.

$10 = 149-139$	$10 = 419-409$	$10 = 719-709$
$10 = 191-181$	$10 = 431-421$	$10 = 797-787$
$10 = 251-241$	$10 = 557-547$	$10 = 821-811$
$10 = 293-283$	$10 = 587-577$	$10 = 839-829$
$10 = 347-337$	$10 = 701-691$	$10 = 929-919$

15. $a>1$ is a square $\Leftrightarrow$ a in canonical form has all even exponents for the primes.

Pf: Suppose a is a square. $\therefore a=n^2$

Let $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = n$. $\therefore n^2 = p_1^{2k_1} \cdots p_r^{2k_r}$, so all exponents are even.

Suppose all exponents of $p_1^{k_1} \cdots p_r^{k_r} = a$ are even.
$\therefore k_i = 2m_i$, some m_i for each k_i
$\therefore a = p_1^{2m_1} p_2^{2m_2} \cdots p_r^{2m_r}$
$= (p_1^{m_1} \cdots p_r^{m_r})^2$

16. (a) $n > 1$ is square free $\Leftrightarrow$ n can be factored into a product of distinct primes.

Suppose n is square free, and let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization.

Suppose any $k_i > 1$. $\therefore k_i \geq 2$, and $\therefore p_i^2$ will divide n, a contradiction of def. of square free. $\therefore$ each $k_i = 1$.

Suppose $n = p_1 \cdots p_r$, each $p_i \neq p_k$.
Suppose n is not square free, and let $a^2 | n$. $\therefore n = xa^2$, x an integer.
Let $a = q_1^{k_1} \cdots q_s^{k_s}$.

$\therefore p_1 \cdots p_r = x\, q_1^{2k_1} \cdots q_s^{2k_s}$ $\therefore q_i | p_1 \cdots p_r$

$\therefore$ By corollary 2 (p. 41), $q_i = p_K$ for some K, $1 \le K \le r$.
After factoring out q_i and p_K, we still have,
$p_1 \cdots p_r = K q_1^{2K_1} \cdots q_i \cdots q_s^{2K_s}$, so that $q_i \mid p_1 \cdots p_r$. But the original factorization $p_1 \cdots p_r$ was unique, and q_i was factored out.
$\therefore$ q_i can't divide the remaining factorization. $\therefore$ n must be square free.

(b) Every $n > 1$ is the product of a square free integer and a perfect square.

Pf: Let $n = p_1^{K_1} \cdots p_s^{K_s}$ be the canonical form for n. If K_i is odd and $K_i > 1$, then $K_i - 1$ is even. Let $a = p_{r_1}^{K_{r_1}} p_{r_2}^{K_{r_2}} \cdots p_{r_m}^{K_{r_m}}$,
where $1 \le r_i \le s$ and K_{r_i} is odd and $K_{r_i} \ge 1$.
Consider $b = p_{r_1} \cdots p_{r_m}$.
$\therefore$ $a = b\, p_{r_1}^{K_{r_1}-1} p_{r_2}^{K_{r_2}-1} \cdots p_{r_m}^{K_{r_m}-1}$

Also, b is square free, by (a) above.
$p_{r_i}^{k_{r_i}-1} = p_{r_i}^{2x_i}$ since each $k_{r_i}-1$ is even. Let $c = p_{r_1}^{x_1} \cdots p_{r_m}^{x_m}$

$\therefore a = bc^2$

Finally, let $a/n = p_{t_1}^{k_{t_1}} \cdots p_{t_j}^{k_{t_j}}$, where all k_{t_i} are even since a/n has factored out all of the odd exponents in the canonical form of n.
By #15 above, $a/n = d^2$

$\therefore n = bc^2d^2 = b(cd)^2$,
where b is square free.

17. $n = 2^k m$, $n \neq 0$, $k \geq 0$, m odd

Pf: Assume $n > 0$ (if $n < 0$, choose k, m s.t. $-n = 2^k m$, $\therefore n = 2^k(-m)$).

If n is odd, choose $k = 0$, $m = n$.
If n is even, then $n = 2k_1$. Note $k_1 < n$.
If k_1 is odd, choose $k = 1$, $m = k_1$
If k_1 is even, then $k_1 = 2k_2$, so

$n = 2^2 k_2$. Note $k_2 < k_1$.
Continue this process till k_i is odd. $\therefore$ $m = k_i$, $k = i$. Since $k_{i+1} < k_i$, this is a finite process (i.e., ultimately will reach 1 is no other odd integer reached by then).

18.

3, 53	47, 97	107, 157
11, 61	53, 103	113, 163
17, 67	59, 109	131, 181
23, 73	83, 139	149, 199
29, 79	101, 151	173, 223

19. If $n > 0$ is square-full, then $n = a^2 b^3$, $a, b > 0$.

Pf: Let $n = p_1^{k_1} \cdots p_r^{k_r}$. Since n is square-full, $k_i \geq 2$.
Write $p_1^{k_1} \cdots p_r^{k_r} = q_{m_1}^{k_{m_1}} \cdots q_{m_s}^{k_{m_s}} q_{n_1}^{k_{n_1}} \cdots q_{n_t}^{k_{n_t}}$,
where k_{m_i} are odd (so $k_{m_i} \geq 3$), and
k_{n_i} are even, such that
$k_{m_i} = k_j$ and $k_{n_i} = k_w$ (i.e., writing

n so that odd exponents listed first, even exponents listed last).

$\therefore K_{n_i} = 2v_i$, some v_i

$$\therefore n = q_{m_1}^{K_{m_1}} \cdots q_{m_s}^{K_{m_s}} \left(q_{n_1}^{2v_i} \cdots q_{n_T}^{2v_T} \right)$$

$$= q_{m_1}^{K_{m_1}} \cdots q_{m_s}^{K_{m_s}} \left(q_{n_1}^{v_1} \cdots q_{n_T}^{v_T} \right)^2$$

$$\therefore n = q_{m_1}^{K_{m_1}} \cdots q_{m_s}^{K_{m_s}} \left(x^2 \right), \quad x = q_{n_1}^{v_1} \cdots q_{n_T}^{v_T}$$

Since K_{m_i} is odd and ≥ 3, $K_{m_i} - 3$ is even.

$$\therefore n = q_{m_1}^{3} \cdots q_{m_s}^{3} \left(q_{m_1}^{m_1 - 3} \cdots q_{m_s}^{m_s - 3} \right) \left(x^2 \right)$$

Let $m_i - 3 = 2w_i$, $q_{m_1} \cdots q_{m_s} = b$,

$\therefore n = b^3 \left(q_{m_1}^{2w_i} \cdots q_{m_s}^{2w_s} \right) \left(x^2 \right)$. Let $y = q_{m_1}^{w_1} \cdots q_{m_s}^{w_s}$

$\therefore n = b^3 y^2 x^2$. Let $a = yx$,

$\therefore n = a^2 b^3$