Chapter 2 of Number Theory with Computer Applications

by Kumanduri and Romero;

University of Windsor 62-322 Course notes by M. Hlynka. and W.L. Yee

Let $\mathbb{Z}$ denote the integers $\{0, \pm 1, \pm 2, \dots\}$.

DEFINITION 2.2.1: Let $a, b \in \mathbb{Z}$. We say a divides b (denoted $a|b$) if there exists $c \in \mathbb{Z}$ such that $ac = b$. We also say a is a *divisor* of b or b is divisible by a. If a does not divide b, write $a \nmid b$.

Note: 0 is divisible by all integers. Here $0|0$ makes sense.

Note: $1|5, 5|5, (-1)|5, (-5)|5$.

Problem MH2.1. What are the (positive) divisors of 100?

$100 = 2^2 \times 5^2$ so its divisors are numbers of the form $2^a \times 5^b$ where $a = 0, 1, 2$ and $b = 0, 1, 2$. That is, $1, 2, 4, 5, 10, 20, 25, 50, 100$.

Problem MH2.2. What are the (positive) divisors of 101? prime

$1, 101$

Lemma 2.1.3

Let a, b, c, x, y be integers.

a. If $a|b$ and $x|y$, then $ax|by$.

b. If $a|b$ and $b|c$, then $a|c$.

c. If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

d. If $a|b$ and $a|c$ then $a|(bx + cy)$. (If $a|b$ and $a|c$, then $a|(b - c)$.)

Proof.

(a only, b will be an exercise, see text for c,d)

a) $ac = b$ and $xd = y$ so $ax(cd) = by$ and thus $ax|by$. ■

Definition: 2.1.4: A positive integer $p > 1$ is *prime* if its only positive divisors are 1 and p. If a positive integer $n > 1$ is not prime, it is *composite*.

Note: 1 is neither prime nor composite.

Note: 2 is the only even prime.

Note: The primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, \ldots$

Well Ordering Principle: Every nonempty set of positive (or nonnegative) integers contains a smallest element. (Note that this is not true for real or rational numbers.)

Division Theorem: Given integers $a > 0$ and $b > 0$, there exist unique q, r such that

$$a = bq + r \text{ with } 0 \leq r < b. \tag{2.1.1}$$

Here r is called the *remainder* and q is the *quotient*.

Proof. Consider the set $S = \{a - bm | m \in \mathbb{Z}\} = \{\ldots a - 2b, a - b, a, a + b, a + 2b \ldots\}$. It contains some positive numbers. Let S^* be the subset of S of values which are nonnegative. By the well ordering principle, there is a smallest nonnegative integer in S^*. Let that number be $r = a - bq$. Show $r < b$ and that q, r are unique.

Suppose $r \geq b$. Then $0 \leq r - b$. But $r - b = a - b(q + 1) \in S^*$ so r is not the smallest nonnegative value. Contradiction. So $r < b$.

Suppose q_1, r_1 and q_2, r_2 both satisfy (2.1.1) then $a = bq_1 + r_1 = bq_2 + r_2$ so $b(q_1 - q_2) = r_2 - r_1$. If $q_1 \neq q_2$, then $|b(q_1 - q_2)| \geq b$ while $|r_2 - r_1| < b$. Contradiction. So $q_1 = q_2$ and thus $r_2 = r_1$. ■

EXAMPLE: (p.13, #9) Show that a perfect square is never of the form $3k + 2$ for any k.

Solution: Let n^2 be the square of an integer. Divide n by 3 to get $n = 3q + 0$ or $n = 3q + 1$ or $n = 3q + 2$. Square both sides to get

$n^2 = 9q^2 + 0 = 3s_1 + 0$ or $n^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3s_2 + 1$ or $n^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3s_3 + 1$. By uniqueness of the division theorem, n^2 can never be of the form $3k + 2$.

MH2.4. Is it true that 3 never divides $n^2 + 1$ for any positive integer n? Explain.

Yes. n^2 is of the form $3k$ or $3k + 1$, so $n^2 + 1$ is of the form $3k + 1$ or $3k + 2$,

neither of which is divisible by 3.

MH2.5. We know the series $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges. Show that $\sum_{k=1}^{n} \frac{1}{k}$ is never an integer for $n > 1$.

Proof: Let 2^N be the greatest power of 2 less than or equal to n. Let $M = 3\times5\times7\times\cdots\times(2m+1)$ where $2m+1$ is the largest odd number less than or equal to n. Then $\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{2^N}+\cdots+\frac{1}{n}\right)2^{N-1}M = \text{sum of integers} + \frac{M}{2}$ is not an integer. Therefore $1+\frac{1}{2}+\cdots+\frac{1}{n}$ is not an integer.

Exercises: p. 13 #2,3,8,21,22,23,25.

Example: p. 13 # 2) Prove:

a) If $a|b$ and $b|c$ then $a|c$.
$ak = b$ and $b\ell = c$ so $ak\ell = c$ so $a|c$.

b) If $a|b$ and $a|c$, then $a|mb+nc$ for all integers m, n.
$ak = b$ and $a\ell = c$ so $m(ak)+n(a\ell) = mb+nc$ so $a(mk+n\ell) = mb+nc$ so $a|mb+nc$.

c) If $a|b$, then $a|kb$ for every integer k.
$ac = b$. Then $a(ck) = kb$ for every integers k so $a|bk$ for every integer k.

Example: p.13 #3) What condition must a and b satisfy so that $a|b$ and $b|a$?
$a|b$ so $ac = b$ for some integer c. $b|a$ so $bd = a$ for some integer d. Then $a = bd = acd$ so $a(1-cd) = 0$. So either $a = 0$ or $cd = 1$. If $a = 0$, $0|b$ implies $b = 0k = 0$ so $a = b = 0$. If $cd = 1$, then $c = d = 1$ in which case $a = b$ or $c = d = -1$ in which case $a = -b$.

Example: p. 13 # 8) Show that when n is odd, n^2-1 is a multiple of 8.
$n = 2k+1$ for some integer k. Then $n^2-1 = (2k+1)^2-1 = 4k^2+4k = 4k(k+1)$. $k(k+1)$ is even since it is a product of two consecutive integers so one is even one is odd. Therefore n^2-1 is divisible by $4\times2 = 8$.

Example: p. 14 # 21) For any prime p, show that p divides the binomial coefficients $\binom{p}{k}$ for $k = 1, \ldots, p-1$.
$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)(p-2)\cdots2\cdot1}{k!(p-k)!}$. The numerator is divisible by p. The denominator is not divisible by p for $k = 1, \ldots, p-1$. Therefore $\binom{p}{k}$ is divisible by

p.

Example: p. 14 # 22) Show that $6|n^3 - n$ for all integers n. Does $4|n^4 - n$ for all integers n?

$n^3 - n = n(n^2 - 1) = (n-1)n(n+1)$ is the product of three consecutive integers. Therefore at least one of them is even and one of them is divisible by 3. Therefore it is divisible by 6.

$2^4 - 2 = 14$ which is not divisible by 4.

Example p. 14 # 23) Show that $5|n^5 - n$ for all integers n. (Actually, $n^5 - n$ is a multiple of 30.) Prove this assertion.

$(-x)^5 - (-x) = -(x^5 - x)$ so it suffices to prove the result for all non-negative integers. We use induction. Base case: $n = 0$: $0^5 - 0 = 0$ is divisible by 5.

Inductive hypothesis: For $n = k$, $n^5 - n$ is divisible by 5.

Inductive step: For $n = k+1$, $(k+1)^5 - (k+1) = k^5 + \binom{5}{1}k^4 + \binom{5}{2}k^3 + \binom{5}{3}k^2 + \binom{5}{4}k + 1 - (k+1)$. By the induction hypothesis, $k^5 - k$ is divisible by 5. By Exercise # 21), $\binom{5}{r}$ is divisible by 5 for $r = 1, \ldots, 4$. Therefore $(k+1)^5 - (k+1)$ is divisible by 5. By induction, $n^5 - n$ is divisible by 5 for every non-negative integer n, and hence for every integer n.

Example p. 14 # 25) The Fibonacci numbers are defined by $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Which Fibonacci numbers are even? Which are multiples of 3 and 5?

$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots$

Every third Fibonacci number is divisible by $F_3 = 2$.

Proof: O O E O O E ...

Every fourth Fibonacci number is divisible by $F_4 = 3$.

Every fifth Fibonacci number is divisible by $F_5 = 5$.

Proof by induction: Base case: $F_5 = 5$ is divisible by 5. Inductive hypothesis:

F_{5n} is divisible by 5. Inductive step:

$$\begin{aligned} F_{5n+5} &= F_{5n+4} + F_{5n+3} = F_{5n+3} + F_{5n+2} + F_{5n+2} + F_{5n+1} \\ &= F_{5n+2} + F_{5n+1} + 2F_{5n+1} + 2F_{5n} + F_{5n+1} \\ &= F_{5n+1} + F_{5n} + 4F_{5n+1} + 2F_{5n} = 5F_{5n+1} + 3F_{5n} \end{aligned}$$

which is divisible by 5 since by the inductive hypothesis F_{5n} is divisible by 5.
In general: can show that every d^{th} number is divisible by F_d by induction.
$F_{kd+d} = F_d F_{kd+1} + F_{d-1} F_{kd}$

Definition: (p. 11) If x is a real number, the greatest integer function (or the floor function) $\lfloor x \rfloor$ is the largest integer less than or equal to x. The ceiling function $\lceil x \rceil$ is the smallest integer greater than or equal to x.

Example: $\lfloor 3 \rfloor = 3$, $\lfloor 3.7 \rfloor = 3$, $\lfloor -2.8 \rfloor = -3$.
$\lceil 3 \rceil = 3$, $\lceil 3.7 \rceil = 4$, $\lceil -2.8 \rceil = -2$

Note: In the Division Theorem, $a = bq + r$, where $q = \lfloor a/b \rfloor$.
Example: Exercise 2.1.14 (page 14), Find the number of multiples of d in the closed interval $[n, m]$, where $d, m, n >$ are positive integers.
Solution: There are $\lfloor n/d \rfloor$ multiples of d in the half open interval $(0, n]$. There are $\lfloor (m-1)/d \rfloor$ multiples of d in the open interval $(0, m)$. So there are $\lfloor n/d \rfloor - \lfloor (m-1)/d \rfloor$ multiples of d in the interval $[m, n]$.

Exercises: p. 14, #13,15,16,19
Exercise p. 14 # 13) Suppose a and b are two real numbers. Give a formula for the number of integers in (a, b) using the floor and ceiling functions. Exercise: similarly, derive formulas for the number of integers in the half-open intervals $(a, b]$ and $[a, b)$.
First suppose $a, b > 0$. # of integers in $(0, b) = \begin{cases} \lfloor b \rfloor = \lceil b \rceil - 1 \text{ if } b \notin \mathbb{Z} \\ b - 1 = \lceil b \rceil - 1 \text{ if } b \in \mathbb{Z} \end{cases}$
# of integers in $(0, a] = \lfloor a \rfloor$

Therefore # of integers in $(a, b) = (0, b) \setminus (0, a]$ is $\lceil b \rceil - 1 - \lfloor a \rfloor$.

Formula still holds for negative integers by translation.

Exercise p. 14 # 15) Find the number of integers less than or equal to 400 that are divisible by 3, by 5, and by 15.

Divisible by 3: $\lfloor 400/3 \rfloor = 133$

Divisible by 5: $\lfloor 400/5 \rfloor = 80$

Divisible by 15: $\lfloor 400/15 \rfloor = 26$

Exercise p. 14 # 16) Determine the number of integers between 200 and 400 divisible by 3, by 7, and by 3 or 7.

The number of positive numbers between 1 and 199 divisible by 3 is $\lfloor 199/3 \rfloor = 66$

The number of positive numbers between 1 and 400 divisible by 3 is $\lfloor 400/3 \rfloor = 133$

Therefore the number of positive integers between 200 and 400 divisible by 3 is $133 - 66 = 67$.

The number of positive numbers between 1 and 199 divisible by 7 is $\lfloor 199/7 \rfloor = 28$

The number of positive numbers between 1 and 400 divisible by 7 is $\lfloor 400/7 \rfloor = 57$

Therefore the number of positive integers between 200 and 400 divisible by 7 is $57 - 28 = 29$.

The number of positive integers between 200 and 400 divisible by 3 and 7 $\lfloor 400/21 \rfloor - \lfloor 199/21 \rfloor = 19 - 9 = 10$.

Therefore the number of integers between 200 and 400 divisible by 3 or 7 is # divisible by 3 + # divisible by 7 - # divisible by both 3 and 7 $= 29+67-10 = 86$.

SECTION 2.2 Primes (p. 15)

A prime number p is a positive integer greater than 1 whose only positive divisors are 1 and p itself.

Proposition 2.2.1 (p. 16)

Every positive integer n can be factored into a product of prime numbers of the form $n = p_1^{a_1} \dots p_k^{a_k}$.

Proof: Suppose, by contradiction, there are positive integers which cannot be factored into a product of primes. Let n be the smallest such number. n

cannot be prime as it isn't a product of one prime, so $n = ab$ for some numbers $1 < a, b < n$. Since $a, b < n$, therefore a and b are products of primes. Thus $n = ab$ is a product of primes, contradiction. Therefore every positive integer n can be factored into a product of primes.
Example $180 = 2^2 3^2 5^1$.

Theorem 2.2.2 (Euclid): (p. 16) There are infinitely many primes.
Proof. We will prove this by contradiction. Assume that there are only finitely many primes $p_1 < \cdots < p_k$. Here p_k is the largest prime. Consider $a = p_1 \cdots p_k + 1 > p_k$.
Case 1: a is prime. This contradicts the fact that p_k is the largest prime.
Case 2: $a = p_1 \cdots p_k + 1$ is not prime. But a is is not divisible by any prime $p_1, \ldots, p_k$ (remainder when you diide a by p_i is 1) so a must be divisible by some prime $p > p_k$. This contradicts the fact that p_k is the largest prime.
So for both Case 1 and Case 2, we have a contradiction.
Thus there are infinitely many primes. ■

Proposition 2.2.3 (Primality Test): (p. 17)
A number n is prime if it is not divisible by any prime q, where $1 < q \leq \sqrt{n}$.
Proof. If n is composite, then $n = ab$. If both $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > n$. Thus at least one of a or b must be less than or equal to $\sqrt{n}$. So any composite number n is divisible by a factor which is less than or equal to $\sqrt{n}$. If there is no such factor, then n is prime. ■
Example: Is 101 prime? First $10 < \sqrt{101} < 11$. We can easily check that 101 is not divisible by 2,3,5,7 so it must be prime.

SIEVE of Eratosthenes

Find all primes less than 60.
Method: (1)Write the numbers in an array.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

(2)Cross out all multiples of 2,3,4,5,6,... other than themselves. Stop when the number is less than $\sqrt{60}$

(3) Whatever is left (> 1) must be prime. See list.

1	2	3	$*$	5	$*$	7	$*$	$*$	$*$
11	$*$	13	$*$	$*$	$*$	17	$*$	19	$*$
$*$	$*$	23	$*$	$*$	$*$	$*$	$*$	29	$*$
31	$*$	$*$	$*$	$*$	$*$	37	$*$	$*$	$*$
41	$*$	43	$*$	$*$	$*$	47	$*$	$*$	$*$
$*$	$*$	53	$*$	$*$	$*$	$*$	$*$	59	$*$

Definition: Let $\pi(x)$ be the number of primes less than or equal to x.

Note: For example, $\pi(60) = 17$.

Prime Number Theorem: (p. 22) $\pi(x) \sim \dfrac{x}{\ln x}$. i.e. $\lim_{x\to\infty} \dfrac{\pi(x)}{x/\ln x} = 1$.

(Legendre: conjectured $\pi(x) \sim \frac{x}{\ln x + B}$ where $B = -1.08366$; Gauss: conjectured $\pi(x) \sim \frac{x}{\ln x}$; Hadamard, de la Vallee Poussin: independent proofs using ideas of Riemann in particular the Riemann zeta function; Erdos and Selberg: elementary proof)

Property 2.2.9. There are arbitrarily large gaps in the sequence of prime numbers.

Proof. If we want a gap of at least $k - 1$, consider

$$k! + 2, k! + 3, \ldots, k! + k.$$

These are all composite, divisible by $2, 3, \ldots, k$ respectively. ■

Notes:

(1) Mersenne numbers are of the form $2^p - 1$. If this is prime, then it is called a *Mersenne prime*. For example, $2^{31} - 1$ is a Mersenne prime. It is unknown whether there are infinitely many Mersenne primes.

(2) Twin primes differ by 2. For example, (11,13) and (29,31) are two pairs of twin primes. The famous 1846 Twin Prime Conjecture states that there are infinitely many twin primes.

April 17, 2013: Yitang Zhang announced a proof for some $N < 70$ million there are infinitely many pairs of primes that differ by N.

April 14, 2014: bound on N reduced to 246. Assuming the generalized Elliott-Halberstam conjecture, bound on N reduced to 6.

(3) Bertrand's conjecture. There is always a prime between n and $2n$ for large n. Proved in 1852 by Chebyshev.

(4) Goldbach's conjecture 1742. Every even number greater than 5 is the sum of two odd primes.

Exercises: (p.24) #1, 6, 7, 8, 9, 10.

Exercise p.24 # 1) In the Sieve of Eratosthenes, when we reach the stage of deleting the multiples of a prime p, what is the first multiple of p that is still in the table?

p

Exercise p. 24 # 5) What are possible remainders when an odd prime is divided by 4? Show that the product of numbers of the form $4k+1$ is again of the form $4k+1$.

$4k$ and $4k+2$ are even. Odd primes are of the form $4k+1$ and $4k+3$.

$(4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_1 + 4k_2 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ so an arbitrary product of numbers of the form $4k+1$ is also of the form $4k+1$.

Exercise p. 24 # 6) Prove there are infinitely many primes of the form $4n+3$. Suppose there are only finitely many primes of that form, $p_1, \ldots, p_i$, excluding 3. Consider $N = 4p_1p_2 \cdots p_i + 3$. By the previous exercise, N cannot be a product of primes of the form $4k+1$, so there must be a prime p of the form $4k+3$ dividing

N. N is not divisible by 3 since none of the p_j are 3, so $p \neq 3$.. $p \neq p_1, \ldots, p_i$ since the remainder when you divide N by p_j is $3 < p_j$. But $p_1, \ldots, p_i$ was the set of all primes other than 3 of the form $4k+3$–contradiction. Therefore there are infinitely many primes of the form $4k+3$.

Exercise p. 25 # 9). Compute the values of the polynomials $f(x) = x^2 + x + 41$ for integral values of x satisfying $-20 \leq x \leq 20$. For which values do they give prime numbers? Does it always give prime numbers for different values of x?

x	$f(x)$
-20	421
-19	383
-18	347
-17	313
-16	281
-15	251
-14	223
-13	197
-12	173
-11	151
-10	131
-9	113
-8	97
-7	83
-6	71
-5	61
-4	53
-3	47
-2	43
-1	41

x	$f(x)$
0	41
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151
11	173
12	197
13	223
14	251
15	281
16	313
17	347
18	383
19	421
20	461

All prime.

$f(41)$ is divisible by 41 and composite:

$41^2 + 41 + 41 = 41 \times 43$

Method 2: $x^2 + x + 41 = (x-1)(x+2) + 43$ is divisible by 43 when $x = 44$ or 41.

Check: $44^2 + 44 + 41 = 43 \times 47$

$41^2 + 41 + 41 = 41 \times 43$

Exercise p. 25 # 10) Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0$ where $n \geq 1$ and $a_n \neq 0$. Show that if $a_0 \neq 1$, then there exists an integer x such that $f(x)$ is composite. If $a_0 = 1$, can you prove that $f(x)$ cannot be prime for all x?

Note that $f(ka_0)$ is divisible by a_0 for all $k \in \mathbb{Z}$. If $a_0 = 0$, then $f(0) = 0$ is not prime. Otherwise, $f(x)$ diverges as $x \to \infty$ so $f(ka_0)$ is a multiple of a_0 not equal to a_0 for large enough k. Then $f(ka_0)$ is composite.

If $a_0 = 1$, there is some b such that $f(x) = (x-b)g(x) + c$ where $c \neq 1$. (This is true since $c = f(b)$.) Then $f(b + kc) = kcg(b + kc) + c$ is divisible by c and composite for big enough k.

2.3 Unique Factorization

Fundamental Theorem of Arithmetic:

The factoring of any positive integer n into primes is unique apart from the order of the primes.

PROOF: See p. 27 of textbook.

Lemma 2.3.1: Let $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$. A positive integer b divides a iff $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ where $0 \leq b_i \leq a_i$ for $i = 1, \ldots, k$.

PROOF: See p. 28 of textbook.

Definition: Let $n > 0$. Let $\nu(n)$ =number of positive divisors of n (including 1 and n).

Examples: $\nu(3) = 2$, $\nu(11) = 2$, $\nu(12) = 6$ (divisors are 1,2,3,4,6,12)

Propositions 2.3.2

Let n be a positive integer with prime factorization $n = p_1^{e_1} \ldots p_k^{e_k}$. The number

of positive divisors of n is

$$\nu(n) = (e_1 + 1) \cdots (e_k + 1).$$

Proof. Every divisor has the form $p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$, where $0 \leq d_i \leq e_i$, $i = 1 \ldots, k$. Thus there are e_i+1 possible values of d_i, for $i = 1, \ldots, k$. Thus the total number of choices is the product

$$\nu(n) = (e_1 + 1) \cdots (e_k + 1).$$

■

EXAMPLE: $12 = (2^2)(3^1)$. Thus $\nu(12) = (2 + 1)(1 + 1) = 6$.
$225 = 15^2 = 3^2 5^2$. Thus $\nu(225) = (2 + 1)(2 + 1) = 9$.

Property 2.3.4 Let a and b be integers. If p is a prime number such that $p|ab$, then $p|a$ or $p|b$.
Proof: Let $a = p_1^{a_1} \cdots p_k^{a_k}$, $b = q_1^{b_1} \times q_r^{b_r}$ be prime factorizations of a and b. $pc = ab = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_r^{b_r}$. Since prime factorizations are unique, $p = p_i$ for some i or $p = q_j$ for some j or both. Then $p|a$ or $p|b$.

Proposition 2.3.5 The number $\sqrt{2}$ is irrational.
Proof. Assume that $\sqrt{2}$ is rational and $\sqrt{2} = a/b$ where a/b is reduced to its lowest terms. Then $2 = \dfrac{a^2}{b^2}$ so $2b^2 = a^2$. Now 2 is prime and divides a^2. By Prop 2.3.4, $2|a$. So $a = 2c$ for some c, and $a^2 = 4c^2$. Hence $2b^2 = 4c^2$ or $b^2 = 2c^2$. Now 2 is prime and divides b^2 so by Prop. 2.3.4, $2|b$. Now we have that $2|a$ and $2|b$ so a/b is not reduced to its lowest terms. Contradiction. So $\sqrt{2}$ is irrational. ■

Proposition 2.3.8 If p is prime and $p < n$, then the exponent of p in the factorization of $n!$ is $\lfloor \dfrac{n}{p} \rfloor + \lfloor \dfrac{n}{p^2} \rfloor + \lfloor \dfrac{n}{p^3} \rfloor + \ldots$.
Proof. There are $\lfloor \dfrac{n}{p} \rfloor$ multiples of p which are less than or equal to n. But some of these numbers are also multiples of p^2 so they have to be counted more

than once. To do this, we must add $\lfloor \frac{n}{p^2} \rfloor$. Thus multiples of p^2 are included. Similarly we must add $\lfloor \frac{n}{p^3} \rfloor$, etc. The result follows. ■

Eg. What is the largest power of 2 dividing 100!?

$\lfloor \frac{100}{2} \rfloor + \lfloor \frac{100}{4} \rfloor + \lfloor \frac{100}{8} \rfloor + \lfloor \frac{100}{16} \rfloor + \lfloor \frac{100}{32} \rfloor + \lfloor \frac{100}{64} \rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97.$

Therefore 2^{97} is the largest power of 2 dividing 100!.

Exercises: p. 31

#1,2,3,4,5,9,10,12

Exercise p. 31 # 1) Show that a number is square if and only if all the exponents in its prime factorization are even.

If $n = a^2$, let $a = p_1^{a_1} \cdots p_k^{a_k}$. Then $n = a^2 = p_1^{2a_1} \cdots p_k^{2a_k}$ so all the exponents in its prime factorization are even. Conversely, if n is such that all the exponents in its prime factorization are even, then n is of the form $n = p_1^{2a_1} \cdots p_k^{2a_k} = (p_1^{a_1} \cdots p_k^{a_k})^2$.

Locker room problem. In a school ithere are 100 lockers, all shut. A student comes in and opens every door. Next a student comes in and closes every second door. Next a student comes in and visits every third locker, shutting open doors and opening shut doors. Then a student visits every fourth locker, etc. Finally, a student visits just the 100th locker and opens it if it is shut and closes it if it is open. Which lockers are still open at the end of this process?

Do this for 20 lockers. Make a table for which student visits each locker.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	3	2	5	2	7	2	3	2	11	2	13	2	3	2	17	2	19	2
			4		3		4	9	5		3		7	5	4		3		4
					6		8		10		4		14	15	8		6		5
											6				16		9		10
											12						18		20

The lockers that are open at the end of the process are those corresponding to perfect squares: perfect squares have an odd number of factors.

Exercise p. 31 # 2) Determine the set of integers for which the number of

divisors is odd.

Let $n = p_1^{e_1} \cdots p_k^{e_k}$. The number of divisors of n is $(e_1+1)(e_2+1)\cdots(e_k+1)$. Therefore the number of divisors of n is odd if each $e_i + 1$ is odd, i.e. if each e_i is even, i.e. if n is a perfect square.

Exercise p. 31 # 3) Characterize the integers n such that $\nu(n) = 2$ and $\nu(n) = 4$.

$\nu(n) = 2$: $n = p_1^{e_1} \cdots p_k^{e_k}$ then $\nu(n) = (e_1+1)\cdots(e_k+1) = 2$. Since the $e_i \geq 1$, therefore $e_i + 1 \geq 2$ so we must have $k = 1$ and $e_1 = 1$. Thus $n = p_1^1$ is prime.

$\nu(n) = 4$: Since $e_i + 1 \geq 2$ we have either $\nu(n) = (e_1+1)(e_2+1) = 4$ so $e_1 = 1$, $e_2 = 1$ so $n = p_1 p_2$. Or $\nu(n) = (e_1+1) = 4$ so $e_1 = 3$ so $n = p_1^3$.

Exercise p. 31 # 4) Determine the smallest positive integer satisfying $\nu(n) = 6$, $\nu(n) = 20$, and $\nu(n) = 100$.

$\nu(n) = 6$:

n	smallest n
p_1^5	2^5
$p_1^1 p_2^2$	$3 \times 2^2 = 12$

Smallest n: 12

$\nu(n) = 20$:

n	smallest n
p_1^{19}	2^{19}
$p_1^1 p_2^9$	$3 \times 2^9 = 1536$
$p_1^1 p_2^1 p_3^4$	$5 \times 3 \times 2^4 = 240$
$p_1^3 p_2^4$	$= 3^3 \times 2^4 = 432$

Smallest n: 240

$\nu(n) = 100$:

n	smallest n
p_1^{99}	2^{99}
$p_1^1 p_2^{49}$	3×2^{49}
$p_1^3 p_2^{24}$	$3^3 \times 2^{24}$
$p_1^9 p_2^9$	$2^9 \times 3^9 = 10,077,696$
$p_1^1 p_2^1 p_3^{24}$	$5 \times 3 \times 2^{24}$
$p_1^3 p_2^4 p_3^4$	$5^3 \times 3^4 \times 2^4 = 162,000$
$p_1^1 p_2^4 p_3^9$	$5 \times 3^4 \times 2^9 = 207,360$
$p_1^1 p_2^1 p_3^4 p_4^4$	$7 \times 5 \times 3^4 \times 2^4 = 45,360$

Smallest n: $45,360$

Exercise p. 31 # 5) Determine all primes p so that $11p + 1$ is a perfect square.

$n^2 = 11p+1$ so $n^2-1 = (n-1)(n+1) = 11p$. The only factorizations of $11p$ as a product of two numbers are $11p = 1 \times 11p$ and $11p = 11 \times p$. Thus: $n-1 = 1$, $n+1 = 11p$ which has no solution since the first equation gives $n = 2$ while $n+1 = 3 \neq 11p$.

$n-1 = 11$, $n+1 = p$ gives the solution $n = 12$ and $p = 13$ since $12+1 = 13$ is prime.

$n-1 = p$, $n+1 = 11$ gives $n = 10$ but then $n-1 = 9$ is not prime, so there is no solution in this case.

$p = 13$ is the only solution.

Exercise p. 31 # 9) If p is a prime number, determine the sum of all the divisors of p^n.

The divisors of p^n are $1, p, p^2, p^3, \cdots, p^n$. The sum of all the divisors if $1 + p + p^2 + \cdots + p^n = \frac{p^{n+1}-1}{p-1}$.

Exercise p. 31 # 10) Prove that $\sqrt{n}$ is irrational if n is not a perfect square.

If n is not a perfect square, then $n = p^{2k+1}m$ for some prime p and integer m not divisible by p. If, by contradiction, $\sqrt{n}$ is rational, then $\sqrt{n} = \frac{a}{b}$ so that $a^2 = nb^2$. Let $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = q_1^{b_1} \cdots q_r^{b_r}$ be the prime factorizations of a and b. Then $p_1^{2a_1} \cdots p_k^{2a_k} = p^{2k+1} m q_1^{2b_1} \cdots q_r^{2b_r}$. The prime p appears to an even exponent in the left side but an odd exponent in the right side–contradiction. Therefore $\sqrt{n}$ is irrational.

Omit Section 2.4

SECTION 2.5 GCD and LCM

Definition 2.5.1: The greatest common divisor (gcd) of two integers a and b is the largest integer which divides a and b. In other words, d is the positive integer such that if c divides a and b, then c divides d. This gcd is sometimes written as (a, b) or $gcd(a, b)$. Note that $(0, 0)$ is undefined.

Example: $(12, 56) = 4$.

Definition 2.5.4: Two nonzero integers with $(a, b) = 1$ or gcd 1 are said to be *relatively prime.*

Example: $(12, 49) = 1$.

Lemma 2.5.4: (a) $(a, b) = (-a, b)$

(b) $(a, b) = (a, a - b)$

(c)$(a, b) = d \implies (a/d, b/d) = 1$.

Proof. For (a),(c), see text.

(b) Assume $a, b > 0$. Let d_1 divide a and b. Then d_1 divides $a - b$. Let d_2 divide a and $a - b$. Then d_2 divides $b = a - (a - b)$. Thus $\{a, b\}$ and $\{a, a - b\}$ have the same common divisors and hence have the same gcd. ■

Euclidean Algorithm: Given positive integers a and b, we have

$$a = bq_1 + r_1, \quad 0 < r_1 < b \tag{1}$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1 \tag{2}$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2 \tag{3}$$

$$\vdots = \vdots \tag{4}$$

$$r_{j-2} = r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1} \tag{5}$$

$$r_{j-1} = r_jq_{j+1} \tag{6}$$

where $(a, b) = r_j$.

Proof. Apply the division theorem repeatedly. The process stops when the division is exact and the remainder is 0. Now we show that r_j is (a, b). Note that $r_j|r_{j-1}$. From (5), $r_j|r_{j-2}$. Repeating this argument eventually gives the fact that $r_j|r_1$, $r_j|b$ and $r_j|a$. So r_j is a divisor of a and b and thus $r_j \leq (a, b)$. Let $d = (a, b)$. From (1), $d|r_1$. From (2), $d|r_2$. Repeating this argument ultimately gives $d|r_j$. Thus $d \leq r_j$. Hence $(a, b) = d = r_j$. ■

Corollary (Theorem 2.5.6):

For any two integers a and b, there exist integers m and n such that $ma + nb =$

(a, b).

Proof. In step (5) of the Euclidean algorithm, $d = (a, b) = r_j$ can be expressed as a linear combination of r_{j-1} and r_{j-2}. Similarly r_{j-1} can be expressed as a linear combination of r_{j-2} and r_{j-3}. Substituting for r_{j-1} gives r_j as linear combination of r_{j-2} and r_{j-3}. Continuing in this fashion eventually leads to $d = (a, b) = r_j$ in terms of a and b. ■

Example: $a = 963$, $c = 657$. Find the gcd.

Solution:

$$\begin{aligned} 963 &= 657(1) + 306 \\ 657 &= 306(2) + 45 \\ 306 &= 45(6) + 36 \\ 45 &= 36(1) + 9 \\ 36 &= 9(4) \end{aligned}$$

Thus $(963, 657) = 9$.

(b) Express the gcd as a linear combination of 963 and 657.

$$\begin{aligned} 9 &= 45 - 36(1) \\ &= 45 - (306 - 45(6))(1) && = (-1)(306) + 7(45) \\ &= (-1)(306) + 7(657 - 306(2)) && = 7(657) - 15(306) \\ &= 7(657) - 15(963 - 657) && = -15(963) + 22(657). \end{aligned}$$

Example 2.5.5:

Show that $6k + 5$ and $5k + 4$ are relatively prime.

Solution:

$$\begin{aligned} 6k+5 &= (5k+4)(1)+(k+1) \\ 5k+4 &= (k+1)(4)+k \\ k+1 &= k(1)+1 \\ k &= 1(k) \end{aligned}$$

so $(6k+5, 5k+4) = 1$.

Method 2: We observe that $5(6k+5) - 6(5k+4) = 1$. Thus $(6k+5, 5k+4)|1$ so $(6k+5, 5k+4) = 1$.

2000 Putnam Problem: B-2

Prove that the expression

$$\frac{gcd(m,n)}{n}\binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

SOLUTION: $gcd(m,n) = am + bn$ for integers a and b. Thus

$$\frac{gcd(m,n)}{n}\binom{n}{m} = \frac{(am+bn)}{n}\binom{n}{m} = (\frac{am}{n} + b)\binom{n}{m}.$$

However $\frac{am}{n}\binom{n}{m} = \frac{am}{n}\frac{n!}{m!(n-m)!} = a\frac{(n-1)!}{(m-1)!((n-1)-(m-1))!} = a\binom{n-1}{m-1}$ which is an integer. The result follows.

Definition 2.5.8 The *least common multiple* $[a,b]$ of integers a, b is the smallest positive integer that is a multiple of both a and b.

Example: $[12, 18] = 36$.

Proposition 2.5.10 Suppose $a = p_1^{a_1} \dots p_k^{a_k}$ and $b = p_1^{b_1} \dots p_k^{b_k}$, where $a_i \geq 0$, $b_i \geq 0$ for $i = 1, \dots k$. Then

$$\text{(a) } (a,b) = p_1^{min\{a_1,b_1\}} \dots p_k^{min\{a_k,b_k\}}. \tag{7}$$

$$\text{(b) } [a,b] = p_1^{max\{a_1,b_1\}} \dots p_k^{max\{a_k,b_k\}}. \tag{8}$$

Proof. (a) Any divisor of both a and b must be of the form $p_1^{c_1} \dots p_k^{c_k}$ with $c_i \leq a_i$ and $c_i \leq b_i$ for $i = 1, \dots k$. Thus $c_i \leq min\{a_i, b_i\}$ for $i = 1, \dots, k$. Then (7) follows.
(b) Change "divisor" in (a) to "multiple" and make other changes. Then (8) follows. ■

Corollary 2.5.12 $(a, b)[a, b] = ab$.
Example: $18 \times 12 = 216$. $(12, 18) = 6$. $[12, 18] = 36$. $6 \times 36 = 216$.

Corollary 2.5.13 If $a|bc$ and $(a, c) = 1$, then $a|b$.

Definition The gcd of $a_1, \dots, a_n$ is the largest divisor of all n integers. Notation used for the gcd is $(a_1, \dots, a_n)$.

Property: $(a_1, \dots, a_n) = (a_1, \dots, a_{n-2}, (a_{n-1}, a_n))$.

Property: If $d = (a_1, \dots, a_n)$, then d is an integer linear combination of $a_1, \dots, a_n$.
Definition $a_1, \dots, a_n$ are pairwise relatively prime if $(a_i, a_j) = 1$ for every pair $\{i, j\}$ in $\{1, \dots, n\}$.

EXERCISES: (p. 44) # 1abc, 2, 3, 4, 5, 7, 12, 14, 19, 23

Exercise p. 44 #1) Compute the gcd of the following pairs by i) computing their prime factorization and ii) by the Euclidean algorithm
a) (781, 994)
i) $781 = 11 \times 71$, $994 = 2 \times 7 \times 71$ so $(781, 984) = 71$
ii)

$$994 = 781(1) + 213$$
$$781 = 213(3) + 142$$
$$213 = 142(1) + 71$$
$$142 = 71(2)$$

Therefore $(781, 994) = 71$.

b) $(5950, 13300)$

i) $5950 = 2 \times 5^2 \times 7 \times 17$, $13300 = 2^2 \times 5^2 \times 7 \times 19$, so $(5950, 13300) = 2 \times 5^2 \times 7 = 350$

ii)

$$13300 = 5950(2) + 1400$$
$$5950 = 1400(4) + 350$$
$$1400 = 350(4)$$

Therefore $(5950, 13300) = 350$.

Exercise p. 45 #2) Express the gcd as a linear combination of the numbers in question 1).

a) $(781, 994) = 71$

$$\begin{aligned} 71 &= 213 - 142(1) \\ &= 213 - (781 - 213(3))(1) = 781(-1) + 213(4) \\ &= 781(-1) + (994 - 781(1))(4) = 994(4) + 781(-5) \end{aligned}$$

b) $(5950, 13300) = 350$

$$\begin{aligned} 350 &= 5950 - 1400(4) \\ &= 5950 - (13300 - 5950(2))(4) = 13300(-4) + 5950(9) \end{aligned}$$

Exercise p. 45 # 3) Prove that $(n, n+1) = 1$ for all n. For which n does $(n, n+2) = 1$ hold?

$(n, n+1) = (n, n+1-n) = (n, 1) = 1$ from $(a, b) = (a, b-a)$. (Alternatively, d divides the difference $(n+1) - n = 1$ so $d = 1$.)

$(n, n+2) = (n, n+2-n) = (n, 2)$ which is 1 when n is odd.

Exercise p. 45 # 4) Prove that if $(a, b) = 1$, then $(a+b, a-b) = 1$ or 2.

Let $d = (a+b, a-b)$. Then d divides the sum $(a+b) + (a-b) = 2a$ and d

divides the difference $(a+b)-(a-b)=2b$. Thus d divides $(2a,2b)=2$ so $d=1$ or 2.

Exercise p. 45 # 5) Suppose $(a,b)=1$ and $(b,c)=1$. Does this imply $(a,c)=1$?

No. Take $c=a\neq 1$ and $b-=1$. Then $(a,c)=(a,a)=a$ while $(a,b)=(b,c)=1$.

Exercise p. 45 # 7) Show that the numbers $6k+5$ and $7k+6$ are relatively prime for every $k\geq 1$.

Apply the Euclidean algorithm:

$$\begin{aligned} 7k+6 &= (6k+5)(1)+k+1 \\ 6k+5 &= (k+1)(5)+k \\ k+1 &= k(1)+1 \\ k &= 1(k) \end{aligned}$$

Therefore $(6k+5,7k+6)=1$.

Exercise p. 45 # 12) Prove that $6n-1,6n+1,6n+2,6n+3,6n+5$ are pairwise relatively prime.

$(6n-1,6n+1)=(6n-1,6n+1-(6n-1))=(6n-1,2)=1$ since $6n-1$ is odd.

Similarly, $(6n+1,6n+3)=1$, $(6n+3,6n+5)=1$.

$(6n+1,6n+2)=1$ and $(6n+2,6n+3)=1$ by exercise #3)

$(6n-1,6n+2)=(6n-1,6n+2-(6n-1))=(6n-1,3)=1$ since $6n-1$ is not divisible by 3. Similarly, $(6n+2,6n+5)=1$

$(6n-1,6n+3)=(6n-1,4)=1$ since $6n-1$ is odd. Similarly, $(6n+1,6n+5)=1$.

$(6n-1,6n+5)=(6n-1,6)=(-1,6)=1$.

Exercise p. 45 # 14) Give an example of numbers $a_1,\ldots,a_k$ for any k such that $(a_1,\ldots,a_k)=1$, but no two are pairwise relatively prime.

$(6,10,15)=(2\times 3,2\times 5,3\times 5)=1$ but $(6,10)=2$, $(6,15)=3$, and $(10,15)=5$.

In general, let $p_1,\ldots,p_k$ be k distinct primes and let $a_i=\frac{p_1p_2\cdots p_k}{p_i}$. Then

$(a_1, \ldots, a_k) = 1$ and no two a_i are relatively prime.

Exercise p. 45 # 19) Show that $(F_n, F_{n+1}) = 1$ for consecutive Fibonacci numbers F_n and F_{n+1}.

We observe that the gcd is 1 for $n = 1$. For $n > 1$ we use the Euclidean algorithm. Note that for $k > 2$ $F_k = F_{k-1} + F_{k-2}$ where $0 < F_{k-2} < F_{k-1}$. Therefore:

$$\begin{aligned} F_{n+1} &= F_n(1) + F_{n-1} \\ F_n &= F_{n-1}(1) + F_{n-2} \\ \vdots &\quad \vdots \\ F_4 &= F_3(1) + F_2 = F_3(1) + 1 \\ F_3 &= F_2(2) = 1(2) \end{aligned}$$

Therefore $(F_n, F_{n+1}) = 1$.

Omit Section 2.6 (for now)