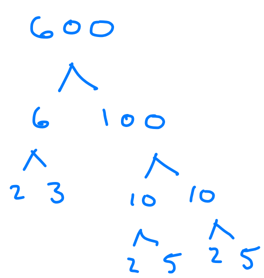
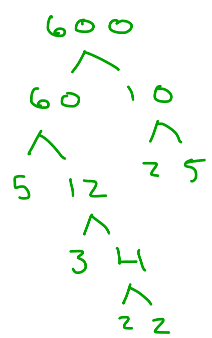
Section 2 – Unique Factorization

Warm-up

① Factor 600 into primes.

② Compare with a neighbor — did you get the same answers?





$600 = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 2 \cdot 5$

$600 = 5 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 5$

only the order is different.
In both cases

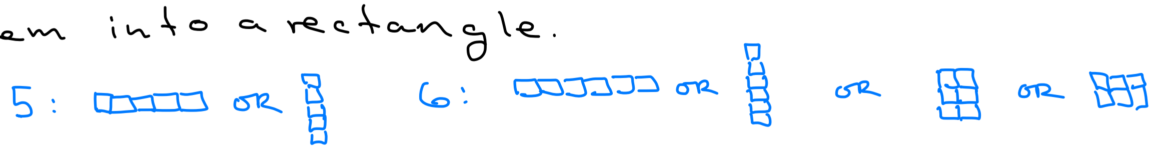
$$600 = 2^3 \cdot 3 \cdot 5^2$$

Def An integer p is called <u>prime</u> if $p \geq 2$ and the only positive divisors of p are 1 and p.

Ex Here are some primes: $2, 3, 5, 7, \ldots, 2^{82,589,933} - 1, \ldots$

largest known as of Jan. 2020. It has 24,862,048 digits!

Visually If you have n blocks, then n is prime if there are only two ways to arrange them into a rectangle.



Def The integers ± 1 are called <u>units</u>. The integers are divided up as follows:

-1, 1

$$\{0\} \cup \{\text{units}\} \cup \{\text{primes}\} \cup \{\underline{\text{composite}} \text{ numbers}\}$$

Lemma 1 If $n \in \mathbb{Z}$ and $n \geq 2$, then n is divisible by some prime.

pf idea

- $n \geq 2 \Rightarrow$ there is a divisor of n that is larger than 1 (b/c n is a divisor of n)
- If p is the smallest divisor of n that is larger than 1, then p is prime

↑ this requires a small proof

$\square$

Lemma 2 (Factorization) If $n \in \mathbb{Z}$ and $n \geq 2$, then n can be written as a product of primes (but maybe just 1 prime).

Ex $6 = 2 \cdot 3$, $8 = 2 \cdot 2 \cdot 2$, $7 = 7$

OPTIONAL

pf of Lemma 2

Suppose the lemma is not true. (It's either true or not!) Then there is some integer larger than 1 that can<u>not</u> be written as a product of primes.

OPTIONAL

Let m be the smallest integer larger than 1 that can not be written as a product of primes

Then

- m is not prime so $m = a, b$ for a, b with $1 < a, b < m$.
- by our choice of m, a and b can be written as a product of primes:

$$a = p_1 \cdots p_k \qquad p_i, q_j \text{ prime}$$
$$b = q_1 \cdots q_\ell$$

- $m = p_1 \cdots p_k q_1 \cdots q_\ell$ so m can be written as a product of primes.

Conclusion: the lemma is true.

$\square$

Theorem 1 - Euclid There are infinitely-many primes. (But we don't know what they are, i.e. no formula.)

pf

Suppose the theorem is not true. Then we can list the primes as $p_1, p_2, \ldots, p_N$. Consider the number

$$m = \overbrace{p_1 \cdot p_2 \cdots p_N}^{a} + 1 \qquad (\text{think } m = 2 \cdot 3 \cdot 5 + 1 = 31)$$

By Lemma 1, m is divisible by some prime, so that prime must be on our list. Suppose $p_k \mid m$ for some $1 \le k \le N$. Notice that

- $m - \overbrace{p_1 p_2 \cdots p_N}^{a} = 1$
- $p_k \mid m$
- $p_k \mid p_1 p_2 \cdots p_N$

By Section 1 – Lemma 2, $p_k \mid 1$, so $p_k = \pm 1$. But, p_k is prime so $p_k \geq 2$. This is a contradiction.

Conclusion: the theorem is true.

$\square$

Warm-up

(a) For which values of $n \in \mathbb{Z}_{>0}$ is $n^2 - 1$ prime?

(b) Repeat for $n^4 - 1$.

Extra 1: Show that if $n^k - 1$ is prime, then $n = 2$.

Extra 2: Show that $n^m - 1$ is never prime when m is composite.

Idea: $n^m - 1 = n^{ab} - 1 = (n^a)^b - 1$. Use Extra 1.

Finding Primes

Options:

1. Guess and check
2. Sieving

① Guess and Check

Ex Is 119 prime?

If not, it has a prime divisor.

p	2	3	5	7
is p a divisor of 119	N	N	N	Y!

$7 \mid 119 \implies$ $\boxed{119 \text{ is NOT prime}}$

Ex Is 139 prime?

p	2	3	5	7	11
is p a divisor of 139	N	N	N	N	N

keep going?!

* suppose 139 is composite. what could its factors be?

$$139 = a \cdot b$$

we now know $a, b \geq 13 \implies 139 \geq 13 \cdot 13 = 169$!!

so $\boxed{139 \text{ is prime}}$

Lemma 4 Let $n \in \mathbb{Z}^+$. If n is composite, then n has some prime divisor p with $p \leq \sqrt{n}$.

very useful

Thus, if n does NOT have a prime divisor p with $p \leq \sqrt{n}$, then n is prime.

OPTIONAL

<u>pf</u> Assume n is composite. Thus

$$n = a \cdot b \quad \text{with} \quad 1 < a, b < n.$$

If $a > \sqrt{n}$ <u>AND</u> $b > \sqrt{n}$, then $n = ab > n$, which is not true. Thus $a \le \sqrt{n}$ <u>OR</u> $b \le \sqrt{n}$.

By Section 2 Lemma 1, a or b has a prime factor p and thus $p \le \sqrt{n}$. Without loss of generality, assume $p \mid a$. Then $p \mid a$ and $a \mid n$, so $p \mid n$. □

<u>Ex</u> Suppose n is a composite two digit number. Explain why n is divisible by one of 2, 3, 5, or 7.

$n < 100 \underset{\text{Lem.4}}{\Longrightarrow}$ n has a prime factor p with $p < 10 \Longrightarrow$ largest possible prime divisor is $\boxed{7}$

(2) <u>Sieving</u> (Sieve of Eratosthenes)

Sieving Handout

Suppose you want to find all primes ≤ 100.

<u>Idea</u>: Remove all composite numbers ≤ 100. The primes are what are left

- $n \le 100$ is composite $\overset{\text{Lem.4}}{\Longleftrightarrow}$ n has a prime divisor $p \le 10$
- to remove composites we need only remove multiples of 2, 3, 5, 7.

Sieving

We want to find all of the prime numbers less than 100.

Idea: list the numbers up to 100 and remove all composite numbers and 1. The primes will be left over.

- If $n \leq 100$, then n is composite $\iff$ n has a prime divisor less that 10.
- So, to remove the composites less than 100, we need only to remove multiples of 2, 3, 5, 7.

Task: cross out all composite numbers, and then circle the prime numbers below.

~~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~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

unit

mult of 2

mult of 3

mult of 5

mult of 7

Follow up: If we wanted all prime numbers less than 400, then we could list the numbers and remove multiples of 2, 3, 5, 7, 11, 13, 17, 19.

stop at 20

20^2

Back to factorization: uniqueness

Lemma 5 Let $p, a, b \in \mathbb{Z}$ with p a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Pf
Note that $\gcd(p,a) = 1$ or p since it must divide p.

- If $\gcd(p,a) = 1$, then $p \mid b$ by Cor 1 of Section 1.
- If $\gcd(p,a) = p$, then $p \mid a$ by def. of gcd. $\square$

Lemma 5 can be generalized to...

Lemma 6 Let $p, a_1, \ldots, a_k \in \mathbb{Z}$ with p a prime. If $p \mid a_1 \cdot a_2 \cdots a_k$, then $p \mid a_i$ for some $1 \le i \le k$.

This leads immediately to...

Lemma 7 Let $p, q_1, \ldots, q_k \in \mathbb{Z}$ all be prime. If $p \mid q_1 q_2 \cdots q_k$, then $p = q_i$ for some $1 \le i \le k$.

Fundamental Theorem of Arithmetic (Unique Factorization Theorem) If $n \in \mathbb{Z}_{\geq 2}$, then n can be written as a product of primes in one and only one way (ignoring order).

pf idea

By lemma 2, n can be written as a prod. of primes. It remains to show this can be done only one way. Suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad \text{with } p_i, q_i \text{ all prime}$$

- $p_1 \mid RHS \Rightarrow p_1 = q_i$ for some $i \geq 1$ (Lemma 7)
  - rearrange the q's so $p_1 = q_1$
  - $\cancel{p_1} p_2 \cdots p_r = \cancel{p_1} q_2 \cdots q_s$
- $p_2 \mid RHS \Rightarrow p_2 = q_i$ for some $i \geq 2$
  - rearrange so $p_2 = q_2$
  - $\cancel{p_2} \cdots p_r = \cancel{q_2} \cdots q_s$
- Continue on. At the end, we find that after rearranging the q's, we have

$$p_1 = q_1, \; p_2 = q_2, \; \ldots, \; p_r = q_r$$

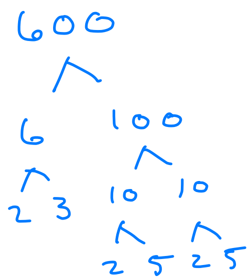
which also implies $r = s$ $\square$

Prime-power Decomposition

When factoring, we often collect multiple copies of each prime into powers. This gives the prime-power decomposition.

↑ def. in book

Ex Find the prime-power decomp. of 600



$$600 = \boxed{2^3 \cdot 3 \cdot 5^2}$$

$$p_1^{e_1} \quad p_2^{e_2} \quad p_3^{e_3}$$

Ex Find the prime-power decomp of 260.
Use this to find $\gcd(600, 260)$

$$260 = \underline{\underline{2^2}} \cdot \underline{\underline{5}} \cdot 13$$

$$600 = \underline{\underline{2^3}} \cdot 3 \cdot \underline{\underline{5^2}}$$

← use minimum exponents

$$\gcd(600, 260) = 2^2 \cdot 5 = \boxed{40}$$

Theorem 3 Let $m, n \in \mathbb{Z}_{>0}$. Let $p_1, \ldots, p_k$ be the primes dividing both m and n. Then

$$m = p_1^{e_1} \cdots p_k^{e_k} \cdot r \qquad \text{and} \qquad n = p_1^{f_1} \cdots p_k^{f_k} \cdot s$$

and $\gcd(m, n) = p_1^{g_1} \cdots p_k^{g_k}$ where $g_i = \min(e_i, f_i)$.

<u>Warm-up</u> Suppose n is a square number and the only prime divisors of n are 2 and 7. What is the smallest number n could be?

so $n = m^2$ for some m.

Idea: If $n = m^2$ and $p | n$, then $p | m$.

<u>Ex</u> Suppose that n is a cube. Prove that every exponent in its prime power decomposition is a multiple of 3.

We know that $n = m^3$ for some m.

Suppose the prime-power decomp of m is

$$m = p_1^{a_1} \cdots p_k^{a_k}.$$

Then,

$$n = (p_1^{a_1} \cdots p_k^{a_k})^3 = p_1^{3a_1} \cdots p_k^{3a_k}.$$

This is the prime-power decomp. of n, and we can see that each exponent is a multiple of 3.