4 Primes

Definition 47. An integer $p > 1$ is a **prime** if its only positive divisors are 1 and p.

Lemma 48. (Euclid's lemma) If $d|ab$ and $(a,d) = 1$, then $d|b$.

Proof. Since $(a,d) = 1$, we can find x, y so that $ax + dy = 1$.
We now see that $b = abx + bdy$ is divisible by d (because $d|ab$). □

Lemma 49. If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof. If $p|a$, then we are done. Otherwise, $p\nmid a$. In that case, $\gcd(a,p) = 1$ because the only positive divisors of p are 1 and p. Our claim therefore is a special case of the previous one. □

Corollary 50. If p is a prime and $p|a_1 a_2 \cdots a_r$, then $p|a_k$ for some $k \in \{1, 2, \ldots, r\}$.

Example 51. This property is unique to primes. For instance, $6|8 \cdot 21$ but $6\nmid 8$ and $6\nmid 21$.
Whereas, $2|8 \cdot 21$ and, indeed $2|8$. Similarly, $3|8 \cdot 21$ and, indeed $3|21$.

Theorem 52. (Fundamental Theorem of Arithmetic) Every integer $n > 1$ can be written as a product of primes. This factorization is unique (apart from the order of the factors).

Proof. Let us first prove, by (strong) induction, that every integer $n > 1$ can be written as a product of primes.

- **(base case)** $n = 2$ is a prime. There is nothing to do.
- **(induction step)** Suppose that we already know that all integers less than n can be written as a product of primes. We need to show that n can be written as a product of primes, too.
  Let $d > 1$ be the smallest divisor of n. Then d is necessarily a prime (because if $a > 1$ divides d, then a also divides n so that $a = d$ because d is the smallest number dividing n).
  If $d = n$, then n is a prime, and we are already done.
  Otherwise, $\frac{n}{d} > 1$ is an integer, which, by the induction hypothesis can be written as the product of some primes $p_1 \cdots p_r$. Then, $n = d p_1 \cdots p_r$.

Finally, let us think about why this factorization is unique. Suppose we have two factorizations

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

By the corollary, each p_i divides one of the q_j's (and vice versa), in which case $p_i = q_j$, so we can cancel common factors until we see that both factorizations are identical. □

Example 53. $140 = 2^2 \cdot 5 \cdot 7$, $2016 = 2^5 \cdot 3^2 \cdot 7$, 2017 is a prime, $2018 = 2 \cdot 1009$, $2019 = 3 \cdot 673$

How can we check that 2017 is indeed prime? Well, none of the small primes $2, 3, 5, 7, 11$ divide 2017. But how far do we need to check? Since $\sqrt{2017} \approx 44.91$, we only need to check up to prime 43. (Why?!)

Example 54. $(p, p+2)$ is a twin prime pair if both p and $p+2$ are primes.

Just making sure. $(2,3)$ is the only pair $(p, p+1)$ with p and $p+1$ both prime. (Why?!)

Some twin prime pairs. $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$, $(101,103)$, …

Largest known one: $\underbrace{3756801695685}_{3 \cdot 5 \cdot 43 \cdot 347 \cdot 16785299} \cdot 2^{666669} \pm 1$ ($200,700$ decimal digits; found 2011)

Twin prime conjecture. Euclid already conjecture in 300 BCE that there are infinitely many twin primes. Despite much effort, noone has been able to prove that in more than 20 centuries.

Recent progress. It is now known that there are infinitely many pairs of primes (p_1, p_2) such that the gap between p_1 and p_2 is at most 246 (the break-through in 2013 due to Yitang Zhang had $7 \cdot 10^7$ instead of 246).

Armin Straub
straub@southalabama.edu