Lecture 2
Euclidean Algorithm, Primes

Euclidean gcd Algorithm - Given \(a, b \in \mathbb{Z}\), not both 0, find \((a, b)\)

- Step 1: If \(a, b < 0\), replace with negative
- Step 2: If \(a > b\), switch \(a\) and \(b\)
- Step 3: If \(a = 0\), return \(b\)
- Step 4: Since \(a > 0\), write \(b = aq + r\) with \(0 \leq r < a\). Replace \((a, b)\) with \((r, a)\) and go to Step 3.

Proof of correctness. Steps 1 and 2 don’t affect gcd, and Step 3 is obvious. Need to show for Step 4 that \((a, b) = (r, a)\) where \(b = aq + r\). Let \(d = (r, a)\) and \(e = (a, b)\).

\[d = (r, a) \Rightarrow d|a, d|r\]
\[\Rightarrow d(aq + r) = b\]
\[\Rightarrow d(a, b) = e\]
\[e = (a, b) \Rightarrow e|a, e|b\]
\[\Rightarrow e|b - aq = r\]
\[\Rightarrow e|r, a\]
\[\Rightarrow e|(r, a) = d\]

Since \(d\) and \(e\) are positive and divide each other, are equal.

Proof of termination. After each application of Step 4, the smaller of the pair \((a)\) strictly decreases since \(r < a\). Since there are only finitely many non-negative integers less than initial \(a\), there can only be finitely many steps. (Note: because it decreases by at least 1 at each step, this proof only shows a bound of \(O(a)\) steps, when in fact the algorithm always finishes in time \(O(\log(a))\) (left as exercise))

To get the linear combination at the same time:

<table>
<thead>
<tr>
<th></th>
<th>43</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>27</td>
<td>0 1</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>1 -1</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
<td>-1 2</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>2 -3</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>-5 8</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[\Rightarrow 1 = -5(43) + 8(27)\]
(Definition) **Prime number**: A prime number is an integer \( p > 1 \) such that it cannot be written as \( p = ab \) with \( a, b > 1 \).

**Theorem 5** (Fundamental Theorem of Arithmetic). Every positive integer can be written as a product of primes (possibly with repetition) and any such expression is unique up to a permutation of the prime factors. (1 is the empty product, similar to 0 being the empty sum.)

**Proof.** There are two parts, existence and uniqueness.

**Proof of Existence (by contradiction).** Let set \( S \) be the set of numbers which cannot be written as a product of primes. Assume \( S \) not empty, so it has a smallest element \( n \) by WOP.

\( n = 1 \) not possible by definition, so \( n > 1 \). \( n \) cannot be prime, since if it were prime it’d be a product with one term, and so wouldn’t be in \( S \). So, \( n = ab \) with \( a, b > 1 \).

Also, \( a, b < n \) so they cannot be in \( S \) by minimality of \( n \), and so \( a \) and \( b \) are the product of primes. \( n \) is the product of the two, and so is also a product of primes, and so cannot be in \( S \) (\( \neq \)), and so \( S \) is empty.

**Proof of Uniqueness.**

**Lemma 6.** If \( p \) is prime and \( p \mid ab \), then \( p \mid a \) or \( p \mid b \).

**Proof.** Assume \( p \nmid a \), and let \( g = (p, a) \). Since \( p \) is prime, \( g = 1 \) or \( p \), but can’t be \( p \) because \( g \mid a \) and \( p \nmid a \), so \( g = 1 \). Corollary from last class (4) shows that \( p \mid b \). \( \square \)

**Corollary 7.** If \( p \mid a_1 a_2 \cdots a_n \), then \( p \mid a_i \) for some \( i \).

**Proof.** Obvious if \( n = 1 \), and true by lemma for \( n = 2 \). By induction, suppose that it holds for \( n = k \). Check for \( n = k + 1 \):

\[
p \mid A \Rightarrow \begin{cases} p \mid A = p \mid a_1 a_2 \cdots a_k \\ p \mid B \Rightarrow p \mid a_i \text{ for some } i \text{ by the induction hypothesis} \\ p \mid A \Rightarrow p \mid a_{k+1} \end{cases}
\]

And so we see that the hypothesis holds for \( n = k + 1 \) as well. \( \square \)
To prove uniqueness, say that we have \( n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \) which is the smallest element in a set of counterexamples. We want to show that \( r = s \) and \( p_1 p_2 \cdots p_r \) is a permutation of \( q_1 q_2 \cdots q_s \).

\( p_1 | n = q_1 q_2 \cdots q_s \), so \( p_i | q_i \) for some \( i \). Since \( p_1 \) and \( q_i \) are prime, \( p_1 = q_i \). Cancel to get \( p_2 \cdots p_r = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s \). This number is less than \( n \), and so not in the set of counterexamples by minimality of \( n \), and so \( r - 1 = s - 1 \) and \( p_2 \cdots p_r \) is a permutation of \( q_1 \cdots q_{i-1} q_{i+1} \cdots q_s \), and so \( r = s \) and \( p_1 p_2 \cdots p_r \) is a permutation of \( q_1 q_2 \cdots q_s \). (\( \checkmark \))

**Theorem 8** (Euclid). *There are infinitely many primes*

*Proof by contradiction.* Suppose there are finitely many primes \( p_1, p_2, \ldots, p_n \), with \( n \geq 1 \). Consider \( N = (p_1 p_2 \cdots p_n) + 1 \). \( N > 1 \), and so by the Fundamental Theorem of Arithmetic there must be a prime \( p_i \) dividing \( N \). Using Euclidean \( \text{gcd} \) algorithm, \( (p_i, (p_1 p_2 \cdots p_n) + 1) = (p_i, 1) = 1 \), and so \( p_i \nmid N \). So, \( p_i \) for any \( i \), and \( p_i \) is a new prime \( \checkmark \).

Note: If you take first \( n \) primes and compute \( a_n = (p_1 p_2 \cdots p_n) + 1 \), it’s an open problem whether all \( a_n (2, 3, 7, 31, 211, 2311, 30031 \ldots) \), are squarefree (no repeated factors).

**Theorem 9** (Euler). *There are infinitely many primes*

*Proof (sketch) by contradiction.* Suppose there are finitely many primes \( p_1, p_2, \ldots, p_m \). Then any positive integer \( n \) can be uniquely written as \( n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \) with \( e_1, e_2 \cdots e_m \geq 0 \). Consider product:

\[
\Sigma = \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} \cdots \right) \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \frac{1}{p_2^3} \cdots \right) \cdots \left(1 + \frac{1}{p_m} + \frac{1}{p_m^2} + \frac{1}{p_m^3} \cdots \right)
\]

where \( \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} \cdots \right) = \frac{1}{1 - \frac{1}{p_1}} < \infty \)

Since each term is a finite positive number, \( \Sigma \) is also a finite positive number. After expanding \( \Sigma \), we can pick out any combination of terms to get

\[
\left(\cdots \frac{1}{p_1^{e_1}} \cdots \right) \left(\cdots \frac{1}{p_2^{e_2}} \cdots \right) \cdots \left(\cdots \frac{1}{p_m^{e_m}} \cdots \right) = \frac{1}{n}
\]

which means that \( \Sigma \) is the sum of the reciprocals of all positive integers. Since all the terms are positive, we can rearrange the terms to get

\[
\Sigma = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} \cdots \frac{1}{n} \cdots = \lim_{n \to \infty} H_n = \infty
\]
and so $\Sigma$ diverges, which contradicts finiteness of $\Sigma (\xi)$. □

**Note:** Euler’s proof shows that $\sum_{p \text{ prime}} \frac{1}{p}$ diverges

Some famous conjectures about primes

**Goldbach Conjecture**
Every even integer $> 2$ is the sum of two primes

**Twin Prime Conjecture**
There are infinitely many twin primes ($n, n + 2$ both prime)

**Mersenne Prime Conjecture**
There are infinitely many Mersenne primes, i.e., primes of the form $2^n - 1$. Note: if $2^n - 1$ is prime, then $n$ itself must be a prime.