10 NUMBER THEORY II

The focus of this section will be Fermat’s Little Theorem, which is also closely related to the final section of the course. We’ll need to do some preparatory work before proving this simple but powerful theorem.

10.1 More about primes

First we prove a generalisation of an earlier result characterising primes: recall Corollary 7.5, that if \( p \in \mathbb{N} \) is prime and \( a, b \in \mathbb{Z} \) with \( p | ab \), then \( p | a \) or \( p | b \).

Lemma 10.1 Let \( p \) be a prime, and let \( a_1, \ldots, a_n \in \mathbb{Z} \).
If \( p | a_1 \ldots a_n \), then \( p \) divides at least one of \( a_1, \ldots, a_n \).

Proof. We use induction on \( n \). Let \( p(n) \) be the statement “if \( p | a_1 \ldots a_n \), where \( a_1, \ldots, a_n \in \mathbb{Z} \), then \( p | a_i \) for some \( i \).”

\( p(1) \) is immediate.
Suppose that \( p(k) \) is true.
Suppose \( a_1, \ldots, a_{k+1} \in \mathbb{Z} \) such that \( p | a_1 \ldots a_{k+1} \). By Corollary 7.5 \( p | a_1 \ldots a_k \) or \( p | a_{k+1} \).
If \( p | a_1 \ldots a_k \), then since \( p(k) \) is true we must have \( p | a_i \) for some \( 1 \leq i \leq k \) and we are done. Otherwise \( p | a_{k+1} \).
Hence \( p(k+1) \) is true. So by induction \( p(n) \) is true for all \( n \).

Theorem 10.2 (Fundamental theorem of arithmetic) Let \( n \in \mathbb{N} \) with \( n \geq 2 \).
Then
(i) \( n = p_1 \ldots p_r \), where each \( p_i \) is prime, and
(ii) any two such expressions for \( n \) differ only in the order of writing.

Remark: The \( p_i \) need not be distinct.

Proof. (i) Suppose false. Then

\[ S = \{ n : n \in \mathbb{N}, n \geq 2, n \text{ cannot be written as a product of primes} \} \neq \emptyset. \]

\( S \) has a minimum element, say \( m \).
Note that \( m \) cannot be prime. Hence \( m = ab \) for some \( a, b \in \mathbb{N} \) with \( 1 < a < m \) and \( 1 < b < m \). By minimality of \( m \), we have \( a, b \notin S \). Hence \( a = p_1 \ldots p_s \) and \( b = q_1 \ldots q_t \) for some \( p_i, q_j \) primes.
Hence \( m = ab = p_1 \ldots p_s q_1 \ldots q_t \), a product of primes, contradicting \( m \in S \). Hence (i) is true after all.

(ii) Suppose false. Hence \( \exists n \in \mathbb{N} \) with \( n \geq 2 \) such that

\[ p_1 \ldots p_s = q_1 \ldots q_t \]
for \(p_i, q_j\) primes, where \(q_1 \ldots q_t\) is not a rearrangement of \(p_1 \ldots p_s\). Cancelling common factors, we may assume that \(1 \neq p_1 \ldots p_s = q_1 \ldots q_t\), where \(\{p_1, \ldots, p_s\} \cap \{q_1, \ldots, q_t\} = \emptyset\).

But \(p_1 | q_1 \ldots q_t\), so by Lemma 10.1 \(p_1 | q_j\) for some \(j\). So \(p_1 = q_j\), a contradiction. Hence (ii) is true after all. 

As an immediate consequence:

**Corollary 10.3** Let \(n \in \mathbb{N}\) with \(n \geq 2\). Then we may uniquely write

\[ n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}, \]

where \(p_1 < p_2 < \cdots < p_r\) are primes and each \(\alpha_j \in \mathbb{N}\).

### 10.2 Fermat’s little theorem

**Example:**

Let \(p = 5\) and \(a \in \{1, 2, 3, 4\}\).

Notice

\[
\begin{array}{c|cccc}
  a^3 & 1 & 2 & 3 & 4 \\
  \hline
  a^3 & 1 & 32 & 243 & 1024 \\
  a^5 - a & 0 & 30 & 240 & 1020
\end{array}
\]

In each case \(5 | a^5 - a\).

This is explained by:

**Theorem 10.4 (Fermat’s little theorem)** Let \(p \in \mathbb{N}\) be prime, and let \(a \in \mathbb{N}\). If \(p \nmid a\), then \(a^{p-1} \equiv 1 \mod p\).

An alternative (equivalent) formulation is:

**Theorem 10.5 (Fermat’s little theorem)** Let \(p \in \mathbb{N}\) be prime, and let \(a \in \mathbb{N}\). Then \(a^p \equiv a \mod p\).

**Proof.** Let \(a \in \mathbb{N}\) and suppose \(p \nmid a\). Then \(a \equiv a_0 \mod p\) for some \(a_0 \in \mathbb{Z}_p \setminus \{0\}\). Consider \(\{1 \odot a_0, 2 \odot a_0, \ldots, (p - 1) \odot a_0\} \subseteq \mathbb{Z}_p \setminus \{0\}\).

\(\gcd(a_0, p) = 1\), so by Lemma 8.3, \(\exists c \in \mathbb{Z}\) such that \(ca_0 \equiv 1 \mod p\).

Hence \(\forall x, y \in \{1, \ldots, p - 1\}\), if \(x \neq y\), then \(ax \not\equiv ay \mod p\) (otherwise \(x \equiv cax \equiv cay \equiv y \mod p\)).

Hence

\[\{1 \odot a_0, 2 \odot a_0, \ldots, (p - 1) \odot a_0\} = \{1, \ldots, p - 1\}\]

Hence

\[(a)(2a)(3a)\ldots((p-1)a) \equiv (a_0)(2a_0)(3a_0)\ldots((p-1)a_0) \equiv 1.2\ldots(p-2)(p-1) \mod p.\]

So \(a^{p-1}(p-1)! \equiv (p-1)! \mod p\).
So \( p|(a^{p-1}(p-1)! - (p-1)!| = (a^{p-1} - 1)(p-1)! \).
But \( p \nmid 1, p \nmid 2, \ldots, p \nmid (p-1) \), so by Lemma 10.1 \( p|(a^{p-1} - 1) \).
Hence \( a^{p-1} \equiv 1 \mod p \). (Hence \( a^p \equiv a \mod p \)). \( \square \)

**Examples:** (i) Find \( 5^{482} \mod 17 \).

By the equivalent formulation of Fermat’s Little Theorem, \( 5^{16} \equiv 1 \mod 17 \).
\[
5^{482} = 5^{16 \times 30 + 2} = (5^{16})^{30}5^2.
\]
Hence \( 5^{482} \equiv (5^{16})^{30}5^2 \equiv 1^{30}5^2 \equiv 25 \equiv 8 \mod 17 \).

(ii) We may use Fermat’s Little Theorem to efficiently show that certain numbers are not prime. In reality this method is most useful for large numbers, using a computer. We demonstrate the method with a small example.

The contrapositive of Fermat’s Little Theorem is that if \( \exists a \in \mathbb{Z} \) such that \( a^n \not\equiv a \mod n \), then \( n \) is not prime.
E.g., 63 is not prime: \( 2^{63} \equiv 2^{60}2^3 \equiv (2^6)^{10}2^3 \). But \( 2^6 \equiv 64 \equiv 1 \mod 63 \), so
\[
2^{63} \equiv 1^{10}2^3 \equiv 8 \not\equiv 2 \mod 63
\]

3