Prime numbers and their properties

Definition 1: An integer $p \geqslant 2$ is said to be **prime**, whenever some $n \in \mathbb{Z}^+$ satisfies $n \mid p$, then $n = 1$ or $n = p$. If $p \geqslant 2$ is not prime, then it is called **composite**.

Various facts about prime numbers can be deduced, some easily, some not so easily.

1. **Fundamental Theorem of Arithmetic**: Every positive integer $n \geqslant 2$ is either prime or the product of primes. Up to the order of the factors, the prime factorization of n is unique, and takes the form $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

   We proved the first sentence in this theorem earlier in the semester, using *strong induction*.

2. There are infinitely many primes.

   Euclid, who lived some 300 years before Christ, gave an elegant proof of this fact, which goes like this: If there were only finitely many primes, the full list would make up the finite set $S = \{p_1, p_2, \ldots, p_N\}$. From these, we can form the number

   $$M = p_1 p_2 p_3 \cdots p_N + 1,$$

   which is not in S, as its construction has given M a magnitude exceeding each element of S. Assuming S contains all the primes, this means M is composite. But, by construction, none of the primes in S can divide M, Our supposition that there are finitely many primes (all contained in S) has allowed us to construct an $M > 2$ that is neither prime nor has a prime factor, contradicting the Fundamental Theorem of Arithmetic. This contradiction nullifies the supposition, which means there are infinitely many primes.

3. If p is prime, then $\forall n \in \mathbb{Z}^+$, $\gcd(n, p) = 1$ or $\gcd(n, p) = p$.

4. If p is prime, $a_1, a_2, \ldots, a_n$ are positive integers, and $p \mid a_1 a_2 \cdots a_n$, then there is at least one a_i for which $p \mid a_i$.

5. Suppose $n \geqslant 2$ is an integer, and suppose that, for each $k = 2, 3, \ldots, \lfloor \sqrt{n} \rfloor$, $k \nmid n$. Then n is prime.

   In particular, in checking that $n = 131$ is prime, we can verify $2 \nmid 131$, $3 \nmid 131$, $5 \nmid 131$, $7 \nmid 131$, and $11 \nmid 131$. Since $\lfloor \sqrt{131} \rfloor = 11$, we need go no further, and can declare 131 is prime. The reason we can stop is that, if there were a larger integer m which divided 131, then the other integer k for which $mk = 131$ would be smaller than $\lfloor \sqrt{131} \rfloor$, and would have been found already.

6. **Prime Number Theorem**. For each integer $n \geqslant 2$ define $\pi(n) = \left| \{p \leqslant n \,|\, p \text{ is prime}\} \right|$. The ratio $\pi(n)/n$ gives the *density* of primes in the set of positive integers up to and including n. This ratio is asymptotic to $1/\ln(n)$ as $n \to \infty$.

   Thus, in the first 10^{1000} integers only about 1/2302.6 integers have been prime. Out to 10^{10000}, only about 1/23026 have been.

7. **Fermat's Little Theorem**. If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

   Moreover, for *every* integer b,

$$b^p \equiv b \pmod{p}.$$

   The consequences of Fermat's Little Theorem include these:
   - When doing arithmetic $\mod p$ (a prime), it becomes much simpler to raise integers to powers. Say our modulus is 11. Then

$$6^{502} = (6^{500})(6^2) = (6^{10})^{50}(36) \equiv (1)(36) \equiv 3 \pmod{11}.$$

   - If p is prime and $p \nmid a$, then the multiplicative inverse of $a \pmod{p}$ is a^{p-2}.
   - If it happens that $\gcd(a, m) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime. As an illustration of this,

$$2^{91} = (2^{12})^7(2^7) \equiv (1)^7(128) \equiv 37 \pmod{91}.$$

     Thus, 91 is composite for, if it were prime, then this last statement would have been of equivalence with $1 \pmod{91}$, not $37 \pmod{91}$.

8. The **Euler totient function** $\varphi(n)$ counts the number of integers $1 \leqslant a \leqslant n$ such that $\gcd(a, n) = 1$. When n is
   - a prime ($n = p$), $\varphi(p) = p - 1$.
   - the power of a prime ($n = p^\alpha$), $\varphi(p^\alpha) = \left(1 - \frac{1}{p}\right) p^\alpha$.

   It is also the case that, whenever $\gcd(a, b) = 1$, $\varphi(ab) = \varphi(a)\varphi(b)$. Taken together with the above, this tells us generally that, given the prime factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \qquad \text{we have} \qquad \varphi(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) n.$$

There is this generalization of Fermat's Little Theorem.

Theorem 1 (Euler's Theorem): For positive integers a, n with $\gcd(a, b) = 1$, $a^{\varphi(n)} \equiv 1 \pmod{n}$.