1 Primes and Factoring

Recall a prime is an integer greater than 1 whose only positive integer divisors are itself and 1. Suppose you have a process that is done and undone by multiplying primes (i.e., done by multiplying primes or powers of primes and undone by factoring a number into its prime divisors (prime factorization)). Are these processes equally easy?

Example:

(a) Multiply 23*47

(b) Multiply 31*52.

(c) Determine the prime factorization of 1711.

(d) Determine the prime factorization of 918.

Example: Is there a largest prime? Why or why not?

2 Encoding with the RSA Method

Definitions:

The (relative) ease of multiplying primes and difficulty of factoring numbers into primes is the foundation of the ____________________ (developed by Rivest, Shamir, & Adleman in the 1970s). This method is a type of public-key cryptography, where anyone can encipher but only someone with a particular key can decipher. To encipher, we first translate our text to numbers called ____________________ (e.g., 00 for space, 01-26 for A through Z), then use __________________________, where we raise to a power E in $\mathbb{Z}_n$. That is for plaintext P_1, P_2, P_3... the ciphertext is C_1, C_2, C_3... where for each i, $C_i \equiv P_i^E \pmod{n}$, $0 \leq C_i < n$. The n that is chosen needs to be a product of 2 distinct primes.

Example: Suppose $n = 33$, $E = 7$ and we want to encipher "HELLO WORLD".

(a) Convert "HELLO WORLD" to plaintext using 00 for space, and 01-26 for A through Z.

(b) Encipher (create ciphertext) using modular exponentiation.

(c) (Optional) Convert back to letters.

Using $n = 33$, we only had space to characterize uppercase letters, a space, and a few other symbols. In general, we may want to distinguish upper and lowercase letters and include numbers and other symbols or keystrokes so larger n's are often necessary to accomodate what we need to be able to say. However, that means our bases (P) and exponents (E) can get much bigger.

Example: Suppose $P = 19$, $E = 41$, $n = 91$. Can we use a calculator to directly translate P to ciphertext C? Why or why not?

Example: Suppose $P = 19$, $E = 41$, $n = 91$. Translate P to ciphertext C.

Example: Suppose $P = 7, E = 53, n = 123$. Translate P to ciphertext C.

Theorem 3.5:

If the integer $n > 1$ is not prime, then n has a prime factor no larger than $\sqrt{n}$.

Why is this helpful?

3 Deciphering with RSA

The exponent D used for deciphering is the smallest possible solution x to the congruence $Ex \equiv 1 \pmod{b}$, where $b = (p-1)(q-1)$ and $\gcd(E, b) = 1$. To solve, we can use the extended Euclidean Algorithm as in Section 3.2.

Example: Using $P = 19$, $E = 41$, $n = 91$:

(a) Find b corresponding to $n = 91$, where b and n are as in the RSA method.

(b) Use the extended Euclidean algorithm to find the value of D corresponding to the constants above.

Why is this method secure?

 Rachel Rupnow. Compiled: February 9, 2023

4 Practicing Everything Together

Suppose $n = 187$, $P = 13$, $E = 73$.

(a) Translate P to ciphertext C.

(b) Find b corresponding to n, where b and n are as in the RSA method.

(c) Use the extended Euclidean algorithm to find the value of D corresponding to the constants above.