Algorithmic number theory
Cryptographic hardness assumptions

Foundations of Cryptography
Computer Science Department
Wellesley College

Fall 2016

Table of contents

One-way functions

- Our private-key cryptographic schemes were based on pseudorandom permutations.
- The resistance to attack of block ciphers such as DES and AES provide some evidence to support the existence of pseudorandom permutations, but we have no proofs.
- It is possible to prove their existence based on one-way functions. But, we don't have an existence proof here either.

Algorithmic number theory

- The goal of this section of the course is to introduce various problems that are believed to be "hard", and to present conjectured one-way functions that can be based on these problems.
- We also study cryptography in a *public-key* setting. In contrast to the private key setting, all known efficient constructions rely on hard mathematical problems from algorithmic number theory. So, guess what?

A note on the meaning of polynomial-time in algorithmic number theory

Recall. An algorithm's running time is measured as a function of the length(s) of its input(s).

Remark. This means that the running time of an algorithm taking as input an integer N is measured in terms of $\|N\|$, the length of the binary representation of N, and not in terms of N itself.

Caution. An algorithm running in time $\Theta(N)$ on input N is thus actually running in an *exponential-time* when measured in terms of its input length $\|N\| = \Theta(\log N)$.

Rithmetic: Some definitions and notation

Definitions

- For $a, b \in \mathbb{Z}$, we say that *a divides b* written $a \mid b$, if there exists an integer c such that $ac = b$.
- If $a \mid b$ and $a > 0$ we call *a divisor of b*. A positive $p > 1$ is *prime* if it has only two divisors: 1 and itself.
- The *greatest common divisor* of two non-negative integers a, b, written $\gcd(a, b)$, is the largest integer c such that $c \mid a$ and $c \mid b$. If $\gcd(a, b) = 1$ we say that a and b are *relatively prime*.

Theorems

- The fundamental *theorem of arithmetic* is that every integer greater than 1 can be expressed uniquely (up to ordering) as a product of primes.
- Let a be an integer and b a positive integer. Then there exists unique integers q, r for which $a = qb + r$ and $0 \leq r < b$.

The Euclidean algorithm and friends

Proposition 8.2. Let a, b be positive integers. Then there exists integer X, Y such that $Xa + Yb = \gcd(a, b)$. Furthermore, $\gcd(a, b)$ is the smallest positive integer that can be expressed this way.

Proof. Consider the set $I \stackrel{\text{def}}{=} \{\hat{X}a + \hat{Y}b \mid \hat{X}, \hat{Y} \in \mathbb{Z}\}$. Note $a, b \in I$, so I certainly contains some positive integers. Let d be the smallest positive integer in I.

We show on the board that $d = \gcd(a, b)$; since d can be written as $d = Xa + Yb$ for some $X, Y \in \mathbb{Z}$, this proves the theorem. □

Remark. Given a and b, the *extended Euclidean algorithm* can be used to compute $\gcd(a, b)$ as well as X, Y for which $Xa + Yb = \gcd(a, b)$.

Two extremely useful corollaries to Proposition 8.2

Proposition 8.3. If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$. In particular, if p is prime and $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof. Board time ...

Proposition 8.4. If $p \mid N$, $q \mid N$, and $\gcd(p, q) = 1$, then $pq \mid N$.

Proof. Bored time?

Reduction modulo N

Definition. Let $a, b, N \in \mathbb{Z}$ with $N > 1$. By Proposition 8.1 there exists unique q, r with $a = qN + r$ and $0 \leq r < N$.
Define $[a \mod N]$ to be equal to this r and note that $0 \leq [a \mod N] < N$.
Definition. We say that *a and b are congruent modulo N*, written $a = b \mod N$, if $[a \mod N] = [b \mod N]$.
Remark. Note that $a = b \mod N$ if and only if $N \mid (a - b)$. Furthermore, $a = [b \mod N]$ implies $a = b \mod N$ but not vice versa.
Remark. Congruence modulo N is an equivalence relation (i.e., reflexive, symmetric, and transitive).
Remark. And it obeys standard rules of arithmetic w.r.t. addition and multiplication. For example, compute $[1093028 \cdot 190301 \mod 100]$.

Multiplicative inverses

Big caution: Congruence modulo N does not, in general, respect division. For example, take $N = 24$. Then $3 \cdot 2 = 6 = 15 \cdot 2 \mod 24$, but $3 \neq 15 \mod 24$.

Definition. If for a given integer b there exists an integer b^{-1} such that $bb^{-1} = 1 \mod N$, we say that b^{-1} is a *multiplicative inverse* of b modulo N and call b *invertible* modulo N.

Remarks. If β is a multiplicative inverse of b modulo N, then so is $[\beta \mod N]$ and any two multiplicative inverses of b are congruent modulo N.

Which integers are invertible modulo N?

Proposition 8.7. Let a, N be integers, with $N > 1$. Then a is invertible modulo N if and only if $\gcd(a, N) = 1$.

Proof. Back to the board.

Example. The extended Euclidean algorithm provides a simple technique for calculating inverse elements. For example, when $a = 11$ and $N = 17$, the algorithm yields

$$(-3) \cdot 11 + 2 \cdot 17 = \gcd(11, 17) = 1$$

from which the inverse of a is easily obtained.