THE EUCLIDEAN ALGORITHM

MATH 195

Recall that

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$$

is a group under multiplication. In particular, every element a has an inverse a^{-1}? But how can it be found, if not by luck?

Euclid's algorithm: Computing the GCD

[This material is covered in §7.5 of the textbook.]

In order to compute the inverse of an element of $\mathbb{Z}/n\mathbb{Z}$, first we must check if $(\mathbb{Z}/n\mathbb{Z})^*$, that is, test if $\gcd(a,n) = 1$. Often this is done (when the numbers are small) by calculating the prime factorization of each number: e.g. $8085 = 3 \cdot 5 \cdot 7^2 \cdot 11$, $7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$, has $\gcd(8085, 7560) = 3 \cdot 5 \cdot 7 = 105$. Indeed, it is enough to know the prime factorization of just one of the numbers; however, when the numbers get large, this method becomes impractical.

There is another algorithm, due to Euclid, as follows:

$$\begin{aligned} 8085 &= 1 \cdot 7560 + 525 \\ 7560 &= 14 \cdot 525 + 210 \\ 525 &= 2 \cdot 210 + 105 \\ 210 &= 2 \cdot 105 \end{aligned}$$

The result of this computation is that 105 is the greatest common divisor of 8085 and 7560.

Fact. The probability that two randomly chose integers are coprime equals $6/\pi^2 = 0.607927\ldots$. That is,

$$\lim_{x \to \infty} \frac{\#\{(a,n) : 0 < a \leq x, 0 < n \leq x, \gcd(a,n) = 1\}}{x^2} = \frac{6}{\pi^2}.$$

For example, the "random" integers 961 and 733 by the Euclidean algorithm gives us:

$$\begin{aligned} 961 &= 1 \cdot 733 + 288 \\ 733 &= 3 \cdot 288 + 49 \\ 228 &= 4 \cdot 49 + 32 \\ 49 &= 1 \cdot 32 + 17 \\ 32 &= 1 \cdot 17 + 15 \\ 17 &= 1 \cdot 15 + 2 \\ 15 &= 7 \cdot 2 + 1 \end{aligned}$$

This is some of the material covered January 31, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

Therefore these integers are indeed coprime!

The Semi-Extended Euclidean Algorithm

We can in fact extend this algorithm to compute the inverse of 733 modulo 961, as follows:

$$\begin{aligned}
0a &\equiv 961 \pmod{961}\\
1a &\equiv 733\\
-(1(1)+0)a = -a &\equiv 228\\
(3(1)+1)a = 4a &\equiv 49\\
-(4(4)+1)a = -17a &\equiv 32\\
(1(17)+4)a = 21a &\equiv 17\\
-(1(21)+17)a = -38a &\equiv 15\\
(1(38)+21)a = 59a &\equiv 2\\
-(7(59)+38) = -451a &\equiv 1 \pmod{961}
\end{aligned}$$

The numbers $1,3,4,1,1,1,7$ are the quotients in the previous calculation (not the remainders).

We write this symbolically as follows: starting with $a_0 = n$, $a_1 = a$, a_{i+1} the remainder of a_{i-1} upon division by a_i, we continue until we reach $a_t = 0$, so we get the decreasing sequence of integers

$$a_0 = n > a_1 > a_2 > \cdots > a_{t-1} > a_t = 0$$

and in this case $a_{t-1} = \gcd(a, n)$. We would like these numbers to decrease with some speed, so we have an algorithm which is reasonably fast.

Claim. $a_{i+1} < a_{i-1}/2$.

Proof. If $a_i \leq a_{i-1}/2$, then $a_{i+1} < a_i \leq a_{i-1}/2$.

Otherwise, $a_i > a_{i-1}/2$, in which case we substract the number directly, i.e. $a_{i+1} = a_{i-1} - a_i < a_i/2$. □

Therefore if we write our numbers in base 2, then the Euclidean algorithm cannot take longer than twice the number of binary digits of our number to complete. Since the binary length differs from the number of decimal digits by the factor $\log_2 10$, this algorithm take only essentially only the logarithm of the number (approximately the length of the number) to complete.

What happens in the extended Euclidean algorithm if the numbers are not coprime? Returning to our example of 8085 and 7560, then we obtain

$$\begin{aligned}
0a &\equiv 8085 \pmod{8085}\\
1a &\equiv 7560\\
-1a &\equiv 525\\
15a &\equiv 210\\
-31a &\equiv 105\\
77a &\equiv 0 \pmod{8085}.
\end{aligned}$$

Notice the significance of the number 77: it is $n/\gcd(a,n) = (3\cdot 5\cdot 7^2\cdot 11)/(3\cdot 5\cdot 7)$.

The Extended Euclidean Algorithm

We can actually keep track of more, if we want more information. Returning to our example ($n = 8085$, $a = 7560$):

$$\begin{aligned} 1n + 0a &= 8085 \\ 0n + 1a &= 7560 \\ 1n - 1a &= 525 \\ -14n + 15a &= 210 \\ 29n - 31a &= 105 \\ -72n + 77a &= 0. \end{aligned}$$

Notice that $72 = a/\gcd(a,n) = (2^3 \cdot 3^3 \cdot 5 \cdot 7)/(3 \cdot 5 \cdot 7)$. The previous line,

$$29n - 31a = 105,$$

is also of some real interest:

Fact. If $a, n \in \mathbb{Z}$, then there are integers x and y such that $xn + ya = \gcd(a,n)$.

For the reader with a bit of group theory, translate the statement as: any subgroup of an infinite cyclic group $\mathbb{Z}$ is cyclic. So, for example, the subgroup $\mathbb{Z}a + \mathbb{Z}n \subset \mathbb{Z}$ must be generated by a single element, namely, $\gcd(a,n)$.