Extended Euclidean Algorithm

- Here is Euclid's algorithm again:
  - $b = q_1 a + r_1, 0 < r_1 < a$
  - $a = q_2 r_1 + r_2, 0 < r_2 < r_1$
  - $r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2$
  - $\vdots$
  - $r_{k-2} = q_k r_{k-1} + r_k, 0 < r_k < r_{k-1}$
  - $r_{k-1} = q_{k+1} r_k$
- Define two sequences x_j and y_j as follows: $x_{-1} = 0, x_0 = 1, y_{-1} = 1, y_0 = 0$

$$x_j = x_{j-2} - q_j x_{j-1} \text{ and } y_j = y_{j-2} - q_j y_{j-1}.$$

- Claim: $r_j = x_j a + y_j b$ for all j. In particular, $\gcd(a, b) = r_k = x_k a + y_k b$.
- Summary: We can calculate $\gcd$'s efficiently and if $\gcd(a, b) = d$ we can effectively find x and y such that $d = xa + yb$.

Example

- a = 114, b = 281
-

j	-1	0	1	2	3	4	5	6
x	0	1	-2	5	-32	37	-69	106
y	1	0	1	-2	13	-15	28	-43

- $53 = (-2) \times 114 + 281, 8 = 5 \times 114 - 2 \times 281, \ldots,$ $1 = 106 \times 114 + (-43) \times 281$

Back to modular arithmetic

- $a \equiv b \mod n$ if n divides $a - b$.
- For each n, this is an equivalence relation on the integers.
- As with 26, addition and multiplication is well-defined for integers mod n.
- As before, we get a ring (all the usual rules of arithmetic work) on the integers mod n.
- The set of equivalence classes is written Z/nZ and when one talks about arithmetic operations, one is talking about addition and multiplication of classes.

Solving equations mod n

Lemma

$ax \equiv b \mod n$ has a solution iff $\gcd(a, n)$ divides b. The solution is unique modulo n if the gcd is 1.

Corollary

If $\gcd(a, n) = 1$ then a has a multiplicative inverse mod n.

Theorem (Chinese remainder theorem)

Suppose that $\gcd(m, n) = 1$. Then for any $a, b \in Z$ there is a unique x mod mn such that $x \equiv a \mod m$ and $x \equiv b \mod n$.

In fact, if $m_i \in Z$ for $i = 1, \dots, n$ and $\gcd(m_i, m_j) = 1$ for $i \neq j$ then for any $a_i \in Z$ for $i = 1, \dots, n$ there is a unique x mod $m_1 m_2 \dots m_n$ such that $x \equiv a_i \mod m_i$ for all i.

Fermat's little theorem

Theorem (Fermat's little theorem)

Suppose that p is prime and p does not divide a. Then

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

- Define the Euler ϕ-function on the set of positive integers by

$$\phi(n) = \text{ the number of } k, 0 < k < n \text{ such that } \gcd(k,n) = 1.$$

Theorem (Euler's theorem)

Suppose $n > 0$ and $\gcd(a,n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n.$$