GCD again

- The greatest common divisor $\gcd$ of two positive integers a and b is the largest number d such that $d|a$ and $d|b$ (d divides a and b). We write $d = \gcd(a, b)$.
- How do we find $\gcd(a, b)$ for $a < b$? Euclid's algorithm:
  - $b = q_1 a + r_1, 0 < r_1 < a$
  - $a = q_2 r_1 + r_2, 0 < r_2 < r_1$
  - $\vdots$
  - $r_{k-2} = q_{k-2} r_{k-1} + r_k, 0 < r_k < r_{k-1}$
  - $r_{k-1} = q_{k-1} r_k$
- Claim: $\gcd(a, b) = r_k$.
- Consider $I = \{xa + yb : x, y \in Z\}$. Claim: If d is the least positive integer in I then $d = \gcd(a, b)$.
- Corollary: There is an x and y such that $\gcd(a, b) = xa + yb$.

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 $d = xa + yb$.

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.