Last time:

▶ Defn: if $xy = 1$ (or $[1]$) then we say $y$ is a (multiplicative) inverse of $x$
  
  ▶ We write $y = x^{-1}$ (exercise: $x^{-1}$ is unique if it exists)

▶ Defn: If $x \in X$ has an inverse $y \in X$, then $x$ is called a unit of $X$

▶ Defn: $X^*$ is the set of units of $X$.
  
  ▶ $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$ \quad $\mathbb{Z}^* = \{1, -1\}$ \quad $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$ \quad $\mathbb{Z}_6^* = \{[1], [5]\}$

▶ Defn: $\varphi(n)$ is the number of units of $\mathbb{Z}_n$.

▶ Claim (Euler’s theorem): if $[a]$ is a unit, then $[a]_{\varphi(m)}^{[b]} := [a^b]_m$ is well defined
  
  ▶ We simplified to Euler’s version 2: if $[a]$ is a unit, then $[a]_{\varphi(m)}^{[\cdot]} = [1]_m$.

Announcements:

▶ There are still a few people who need to take the makeup exam
  
  ▶ limit your discussion of the exam accordingly
  
  ▶ If you haven’t taken the exam yet, don’t go to discussion

▶ Prelim grades coming early next week

▶ Course grade estimates coming shortly thereafter
Claim (Euler’s theorem): if \([a]\) is a unit, then \([a]_{m}^{[b]_{\varphi(m)}} := [a^{b}]_{m}\) is well defined

- We simplified to Euler’s version 2: if \([a]\) is a unit, then \([a]_{m}^{\varphi(m)} = [1]_{m}\).

Fact (Bézout’s identity): For all \(a, b\), there exist \(s\) and \(t\) with \(gcd(a, b) = sa + tb\)

- \(s\) and \(t\) are the “Bézout coefficients” of \(a\) and \(b\)
- Proof is on next homework week

Claim: \([a]_{m}\) is a unit if and only if \(gcd(a, m) = 1\).

- \(a\) is relatively prime to \(b\) means \(gcd(a, b) = 1\) (\(a\) and \(b\) have no common factors)
- \([a]^{-1} = [s]\) where \(gcd(a, m) = sa + tm\)

Claim: \(\varphi(p) = p - 1\) if \(p\) is prime

Claim: \(\varphi(pq) = (p - 1)(q - 1)\) if \(p\) and \(q\) different primes

How to send a message over a public channel without allowing attacker to observe?