Homework

due on Friday, April 1

Read carefully sections 6.1-6.4 in the book. Read the notes about congruences linked on the course page. Solve the following problems.

Problem 1. Use Euclid's algorithm to compute $\gcd(803, 154)$ and find integers λ, μ such that $\gcd(803, 154) = \lambda \cdot 803 + \mu \cdot 154$. Show all your work.

Problem 2. Let n be a positive integer. Consider the set $\mathbb{Z}_n$ of equivalence classes modulo n. Let $x \in \mathbb{Z}_n$.

a) Prove that if x contains an element which is relatively prime to n then all elements in the class x are relatively prime to n.

b) Let $x = [m]$, where m is relatively prime to n. We have proved in class that there exist integers u, w such that $um + wn = 1$. Use this to prove that x has a multiplicative inverse in $\mathbb{Z}_n$.

c) Prove the converse, that if x has a multiplicative inverse in $\mathbb{Z}_n$ then $x = [m]$ for some m relatively prime to n.

d) List all elements in $\mathbb{Z}_{12}$ which have multiplicative inverse.

Problem 3. Find the remainder when 3^{337} is divided by 31. Hint: Use Fermat's Little Theorem.

Problem 4. a) Let p and q be distinct primes numbers. Prove that if $p|m$ and $q|m$ then $pq|m$.

b) Let p and q be distinct prime numbers. Prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq} .$$