

Math 216
Homework 3
Due Fri. Feb. 8

3.1 Fix an integer $n \geq 2$. Prove that the relation on \mathbb{Z} defined by $a \sim b$ if $a \equiv b \pmod{n}$, is an equivalence relation.

3.2 Let us write the elements of \mathbb{Z}_7^\times as $[1]$, $[2]$, $[3]$, $[4]$, $[5]$, $[6]$. Compute the following in \mathbb{Z}_7 .

- (1) $[1][2][3][4][5][6]$
- (2) $[2]^n$, for any n (The answer depends on the class of $n \pmod{3}$.)
- (3) $[3]^n$, for any n . (The answer depends on the class of $n \pmod{?}$.)
- (4) $[a]^6$, for any a .

3.3. In 3.2 parts (1) and (4), what happens if 7 is replaced by a general prime p ? Do some examples, say with $p = 5$ and $p = 11$, and then make two conjectures, saying what you think the analogues of (1) and (4) are for general primes p . Don't worry about proving these yet. The analogues of (1) and (4) are called "Wilson's Theorem", and "Fermat's Little Theorem", respectively.

3.4. Let G be a finite abelian group, and suppose G has exactly one element of order two, call it t . Prove that the product of all the elements of G is t . Use this to prove your conjectural analogue of (1) in 3.3. (Wilson's Theorem.)

3.5. Let G be a finite abelian group, with n elements. Use Lagrange's Theorem to prove that $a^n = e$ for every $a \in G$. Use this to prove your conjectural analogue of (4) in 3.3. (Fermat's Little Theorem.)

3.6. Use Lagrange's theorem for the group $G = \mathbb{Z}_p^\times$ to prove that if -1 is a square mod p then $p = 4k + 1$ for some $k \in \mathbb{Z}$. Use this to show that any prime dividing a Fermat number F_n , $n \geq 1$, is of the form $4k + 1$. Then explain why the second Book proof (bottom of first page of Chapter 1), of the infinitude of primes, actually produces infinitely many primes of the form $4k + 1$. (We have already found infinitely many primes of the form $4k + 3$, on hw 1, but that method did not work for $4k + 1$.)

3.*. (Just for fun, it doesn't count) Try to factor F_5 , F_6 , and F_7 using your calculator. These factorizations were found in 1732, 1880 and 1970, respectively.