

Math 160a - Fall 2002
Lloyd Kilford

Homework set 7
Due: 21st November 2002

1. Let p be a rational prime, and let F be the property that

$$\text{For all } a \in \mathbf{Z}, \left(\frac{a}{p}\right) = -1 \iff a \text{ is a primitive root modulo } p.$$

Show that F holds if and only if p is a Fermat prime.

2. Let n be a composite integer. Show that $(n-1)! \not\equiv -1 \pmod{n}$.
3. Let p be a rational prime. Show that $(p-1)! \equiv -1 \pmod{p}$. Conclude that checking the value of $(m-1)! \pmod{m}$ is a test for the primality of m . Is this a reasonable test? Check that 11 is prime using this test.
4. Why is ideal theory for fields an uninteresting topic?
5. Let n be a rational integer greater than 2. Show that there are no primitive roots modulo 2^n .