

Math 458 quiz October 27, 2009

I hope these questions are short and interesting and neither too easy nor too hard – that’s a difficult combination to arrange. Do what you can in the hour and a quarter you have in class. Turn in your paper, then take the exam home and redo any problems you missed as homework for Thursday.

This is an open book(s) open notes exam (though it’s not clear how much they will help). No internet. Calculators are OK.

- Find the (multiplicative) inverse of 7 modulo 15.
 - Explain why it’s particularly easy to find $a^{-1} \pmod{n}$ when $n \equiv 1 \pmod{a}$.
- Let $\lambda(n)$ be the least integer k such that $a^k \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.
 - Show that $\lambda(n) \leq \varphi(n)$. (Of course φ is Euler’s phi-function.)
 - Is there an n for which $\lambda(n) < \varphi(n)$?
 - Prove that $\lambda(n)$ divides $\varphi(n)$.
Hint: Consider $a^d \pmod{n}$ where $d = \gcd(\lambda(n), \varphi(n))$.

- Consider the polynomial

$$f(x) = (x^2 + 1)(x^4 - 4)$$

- Factor $f(x)$ into irreducibles modulo 2, 7 and 13.
 - Prove that $f(x)$ has a root modulo p for every prime p but has no integral root. Does it have any real roots?
- Find the third smallest unit in the ring $Z[\sqrt{11}]$.
Hint: You don’t need to go very far by trial and error to find one solution to the appropriate Diophantine equation.
 - Conjecture relationships among the assertions that follow (completing them when necessary) and prove what you can.
 - The Diophantine equation $x^2 - 11y^2 = p$ has a solution.
 - $p^{??} \equiv ?? \pmod{11}$.
 - $p \equiv ?? \pmod{??}$