

**MATH 4400/6400**  
**HOMEWORK 2**  
**DUE 1/31/08**

**Instructions:** Math 6400 students should do all the problems. Math 4400 students should do everything but 2(c), 7, and 8.

**Problem 1:** (a) Let  $a$  be an integer  $\geq 2$ . Let  $m$  and  $n$  be positive integers. Show that

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

(b) Let  $c$  and  $d$  be positive integers. Let  $F$  be any field. Show that in  $F[x]$ ,

$$\gcd(x^c - 1, x^d - 1) = x^{\gcd(c,d)} - 1.$$

**Problem 2:** Let  $p$  be an odd prime.

(a) For  $a \in \mathbb{F}_p^*$ , show that  $a$  is a perfect square if and only if  $a^{\frac{p-1}{2}} = 1$ .

(b) Show that there are exactly  $\frac{p-1}{2}$  perfect squares in  $\mathbb{F}_p^*$ .

(c) Extend these statements to finite fields. (There should not be too much work to do here, although you might want to consider  $q = 2^k$  separately.)

**Problem 3:** In this problem, let  $m$  and  $n$  be relatively prime positive integers.

(a) Recall the Chinese Remainder Theorem from algebra. Prove that there is a ring isomorphism

$$(\mathbb{Z}/mn\mathbb{Z}) \rightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

(b) Show that this induces a bijection (actually, an isomorphism of groups)

$$(\mathbb{Z}/mn\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

Explain why this implies that, for  $n$  odd,  $(\mathbb{Z}/2n\mathbb{Z})^*$  is cyclic if  $(\mathbb{Z}/n\mathbb{Z})^*$  is.

(c) Show that  $(\mathbb{Z}/mn\mathbb{Z})^*$  cannot be cyclic if  $m$  and  $n$  are relatively prime integers bigger than 2. (Use part (b); note that  $\phi(m)$  and  $\phi(n)$  are both even!)

**Problem 4:** Let  $a$  be an integer  $\geq 3$ . Show that  $(\mathbb{Z}/2^a\mathbb{Z})^*$  cannot be cyclic. (Hint: show in fact that  $x^{2^{a-2}} \equiv 1 \pmod{2^a}$ , for all odd  $x$ ; you should probably try to do this by induction.)

**Problem 5:** We have seen that for all integers  $a$ ,  $a^p \equiv a \pmod{p}$  if  $p$  is prime. In this problem we investigate the converse.

(a) If  $a^m \equiv a \pmod{m}$  for all integers  $a$ , we say that  $m$  is a *Carmichael number*. Show that 561 is a Carmichael number. (Hint: Factor 561, and use Fermat's little theorem and the Chinese Remainder Theorem.)

(b) Prove *Korselt's criterion*:  $m$  is a Carmichael number if and only if  $m$  is a product of distinct odd primes  $p_i$  all satisfying  $(p_i - 1) | (m - 1)$ . (Feel free to look at Chapter 19 of Silverman's book here, but notice that he leaves some details for you to fill in!)

(c) Show that  $(6k + 1)(12k + 1)(18k + 1)$  is a Carmichael number if all three of the given factors are prime.

*Remark:* In 1994, Alford, Granville, and Pomerance (all three of whom were UGA professors!) showed that for sufficiently large  $n$ , there are at least  $n^{2/7}$  Carmichael numbers less than  $n$ , which demonstrated for the first time that there were infinitely many Carmichael numbers. (The bound has since been improved slightly.)

**Problem 6:** When we proved Euler's theorem in class, we cancelled the product

$$\prod_{\substack{1 \leq x \leq m \\ \gcd(x, m) = 1}} x$$

from both sides. Find a formula for this product, in terms of the prime factorization of  $m$ . (Hint: you should be able to show first that it's  $\pm 1$ .)

**Problem 7:** Show that there is an injective homomorphism  $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$  if and only if  $a|b$ . (I think you should be able to reconstruct the proof by looking at the right pages in Prof. Shifrin's book.)

**Problem 8:** In this problem we investigate the number of solutions to the congruence  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ , where  $p$  is an odd prime. Call this  $n_p$ .

(a) Show that

$$\begin{cases} 0 \leq n_p \leq 2p - 2 & \text{if } p \equiv 3 \pmod{4} \\ 2 \leq n_p \leq 2p & \text{if } p \equiv 1 \pmod{4} \end{cases}$$

(b) Let  $m_p$  be the number of solutions  $(x, y, z)$  to the equation  $x^2 + y^2 + z^2 \equiv 0 \pmod{p}$ . Show that

$$(p - 1)n_p = \begin{cases} m_p - 1 & \text{if } p \equiv 3 \pmod{4} \\ m_p - 2p + 1 & \text{if } p \equiv 1 \pmod{4} \end{cases}$$

(Hint: each solution of the original congruence extends in  $p - 1$  ways to a solution to the new one.)

(c) Chevalley-Waring implies that  $m_p \equiv 0 \pmod{p}$ . So conclude that

$$n_p = \begin{cases} p + 1 & \text{if } p \equiv 3 \pmod{4} \\ p - 1 & \text{if } p \equiv 1 \pmod{4} \end{cases}$$

and hence  $m_p = p^2$  for all  $p$ . (Hint: Compute  $n_p \pmod{p}$  using part (b); you may want to note that  $n_p$  must be even.)

*Remark:* The end of the problem suggests that maybe the best way to do it would have been to prove that  $m_p = p^2$  for all  $p$ , and then to derive  $n_p$  from part (b). If you're getting confused, you might try to do the problem this way instead (for full credit, of course!)