

**MATH 4400**  
**HOMEWORK 2**  
**COMMENTS AND SOLUTIONS**

**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  $F[x]$ ,

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

**Solution:** (a) Let  $d = \gcd(m, n)$ . Clearly  $a^d - 1$  divides  $a^m - 1$  and  $a^n - 1$ . Now let  $b$  be a common divisor of  $a^m - 1$  and  $a^n - 1$ . Then  $a^m \equiv a^n \equiv 1 \pmod{b}$ . We can write  $d = mx + ny$  for some integers  $x, y$ . So  $a^d = a^{mx+ny} = a^{mx}a^{ny} \equiv 1 \pmod{b}$ . So  $b | (a^d - 1)$ . We have shown that every common divisor divides  $a^d - 1$ , so it is the gcd.

(b) This goes the same way; clearly  $x^{\gcd(c,d)} - 1$  divides  $x^c - 1$  and  $x^d - 1$ . Now let  $g(x)$  be a common divisor of  $x^c - 1$  and  $x^d - 1$ . Then  $x^c \equiv x^d \equiv 1 \pmod{g(x)}$ . Writing  $\gcd(c, d) = cr + ds$  for some integers  $r, s$ , we see that  $x^{\gcd(c,d)} \equiv 1 \pmod{g(x)}$ , so  $g(x) | (x^{\gcd(c,d)} - 1)$ . We have shown that every common divisor divides  $x^{\gcd(c,d)} - 1$ , so it is the gcd.  $\square$

**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.

**Solution:** (a) If  $a = b^2$ , then  $a^{\frac{p-1}{2}} = b^{p-1} = 1$ . On the other hand, once we have proved part (b) we know that there are  $\frac{p-1}{2}$  perfect squares, so we already have  $\frac{p-1}{2}$  roots of the polynomial  $x^{\frac{p-1}{2}} - 1$ , so these must be all of the roots. So the converse is true as well.

(b) Squaring is a two-to-one map: there are exactly two solutions to the equation  $x^2 = a^2$ , for all  $a \in \mathbb{F}_p^*$ . This is because  $\pm a$  are both solutions, and there can be no more than two roots of a quadratic polynomial. So the image of the squaring map must have size equal to half the size of  $\mathbb{F}_p^*$ .

*Remark:* It is reasonable to use that  $\mathbb{F}_p^*$  is cyclic to do parts (a) and (b), but it is not necessary, as the above proofs show.

(c) For  $\mathbb{F}_q^*$ , the statements and proofs all extend effortlessly (with  $p$  replaced by  $q$ , of course). But if  $q = 2^k$ , then  $\frac{q-1}{2}$  is not even an integer, so the statements of part (a) and (b) must be modified. What is in fact true is that *every* element of  $\mathbb{F}_{2^k}$  is a square! To see this, note that squaring is a bijection on  $\mathbb{F}_{2^k}$ , because its inverse is the map  $x \mapsto x^{2^{k-1}}$ . (Again, it might be easier to see this by using that  $\mathbb{F}_{2^k}^*$  is cyclic, but it's not necessary.)

*Remark:* In fact, in characteristic  $p$  the  $p$ th power map is an isomorphism  $\mathbb{F}_{p^k} \rightarrow \mathbb{F}_{p^k}$ , sometimes called the *Frobenius automorphism*.  $\square$

**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 and only 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.

**Solution:** (a) The map sends  $\bar{x}$  to  $(\bar{x}, \bar{x})$ . This is well-defined because if  $x \equiv y \pmod{mn}$ , then  $x \equiv y \pmod{m}$  and  $\pmod{n}$ . And it's trivially a homomorphism. Notice that the map makes sense even if  $m$  and  $n$  are not relatively prime; it just won't be a bijection.

To see that the map is a bijection, notice that what it boils down to is the following statement: every element  $(\bar{a}, \bar{b})$  in  $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$  is mapped to by exactly one element of  $(\mathbb{Z}/mn\mathbb{Z})$ . This in turn is equivalent to saying that there is exactly one solution mod  $mn$  to the simultaneous congruences  $x \equiv a \pmod{m}$ ,  $x \equiv b \pmod{n}$ . This is exactly the Chinese Remainder Theorem!

(b) The restriction of the above homomorphism to  $(\mathbb{Z}/mn\mathbb{Z})^*$  is no longer well-behaved under addition (the sum of two units might not be a unit), but it still respects multiplication. So it's a group homomorphism. Notice that it lands in the product of the two unit groups: if  $\gcd(x, mn) = 1$ , then  $\gcd(x, m) = 1$  and  $\gcd(x, n) = 1$ . (Be sure you check this!)

So the restriction is still clearly injective (it's the restriction of an injective map), and now to see that it is surjective, suppose that  $x \equiv a \pmod{m}$  and  $x \equiv b \pmod{n}$ , where  $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$  and  $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ . We know that exactly one solution  $x$  to this equation exists in  $\mathbb{Z}/mn\mathbb{Z}$ , but we have to show that this solution is actually in  $(\mathbb{Z}/mn\mathbb{Z})^*$ . Well, since  $x \equiv a \pmod{m}$ , and  $a$  and  $m$  are relatively prime, then  $x$  and  $m$  are relatively prime. Similarly for  $n$ . So  $\gcd(x, m) = 1$  and  $\gcd(x, n) = 1$ . Suppose  $\gcd(x, mn) \neq 1$ ; then let  $p$  be a prime dividing  $x$  and  $mn$ . Then  $p|m$  or  $p|n$ . WLOG  $p|m$ . But then  $p|\gcd(x, m)$ , a contradiction.

Notice that this implies that  $(\mathbb{Z}/2n\mathbb{Z})^*$  is isomorphic as a group to  $(\mathbb{Z}/n\mathbb{Z})^*$ . (In other words, there is a bijection between the two sets that respects multiplication.) So one group is cyclic if and only if the other one is.

(c) I'm afraid you needed to know here that  $\varphi(m)\varphi(n) = \varphi(mn)$ . Sorry about this. Anyway, notice that every element in  $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$  satisfies  $(a, b)^\ell = 1$ , where  $\ell$  is a common multiple of  $\varphi(m)$  and  $\varphi(n)$ . In particular, note that  $\varphi(m)\varphi(n)/2$  will do as a choice for  $\ell$ , because  $\varphi(m)$  and  $\varphi(n)$  are both even. So let  $\ell = \varphi(mn)/2 = \varphi(m)\varphi(n)/2$ . By the isomorphism in part (b), we have that for all  $x \in (\mathbb{Z}/mn\mathbb{Z})^*$ ,  $x^\ell = 1$ . So  $(\mathbb{Z}/mn\mathbb{Z})^*$  cannot be cyclic, because there is no element of order  $\varphi(mn) = 2\ell$ .  $\square$

**Problem 4:** Let  $a$  be an integer  $\geq 3$ . Show that  $(\mathbb{Z}/2^a\mathbb{Z})^*$  cannot be cyclic.

**Solution:** The hint tells us what to do: in fact we prove that  $x^{2^{a-2}} \equiv 1 \pmod{2^a}$  for all  $x \in (\mathbb{Z}/2^a\mathbb{Z})^*$ . We do this by induction; the base case  $a = 3$  is easily seen (the units are 1, 3, 5, 7 mod 8, all of whose squares are 1 mod 8).

Now suppose the result has been proven for  $a = n$ . Take  $x \in (\mathbb{Z}/2^{n+1}\mathbb{Z})^*$ . By the inductive hypothesis we know that  $x^{2^{n-2}} = 1 + 2^n k$  for some integer  $k$ . Square both sides and consider the result mod  $2^{n+1}$ :

$$x^{2^{n-1}} \equiv (1 + 2^n k)^2 \equiv 1 + 2^{n+1}k + 2^{2n}k^2 \equiv 1 \pmod{2^{n+1}}.$$

The result follows by induction.

Now  $(\mathbb{Z}/2^a\mathbb{Z})^*$  cannot be cyclic, because  $\varphi(2^a) = 2^{a-1}$ , and the result we just proved shows that no element can have an order that large.  $\square$

**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  $a$  and  $m$  is not prime, we say that  $m$  is a *Carmichael number*. Show that 561 is a Carmichael number.

(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  $(p_i - 1) | (m - 1)$ .

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

**Solution:** (a) This was supposed to lead you to the proof of (half of) Korselt's criterion. Here 561 factors as  $3 \cdot 11 \cdot 17$ . Now consider  $a^{561} \pmod{3}$ . If  $3|a$ , then of course this is congruent to  $a$ . Otherwise Fermat's little theorem says that  $a^2 \equiv 1 \pmod{3}$ , so  $a^{560} \equiv 1$ , so  $a^{561} \equiv a$ . Thus for all  $a$  we have proved that  $a^{561} \equiv a \pmod{3}$ . Similarly  $a^{561} \equiv a \pmod{11}$  (because  $10|560$ ), and  $a^{561} \equiv a \pmod{17}$  (because  $16|560$ ). Now the Chinese Remainder Theorem immediately gives that  $a^{561} \equiv a \pmod{561}$ .

(b) First suppose  $m$  is such a product. Then we proceed as we did in part (a), by noting that  $a^m \equiv a \pmod{p_i}$  for all  $a$ , because  $(p_i - 1) | (m - 1)$ . Then the Chinese Remainder Theorem implies that  $a^m \equiv a \pmod{m}$ .

Now for the converse. Let  $m$  be a Carmichael number. First suppose  $p^2 | m$  for some prime  $p$ . Then let  $g$  be a primitive root mod  $p^2$ . The order of  $g \pmod{p^2}$  is  $p(p - 1)$ . But  $g^m \equiv g \pmod{p^2}$ , so  $g^{m-1} \equiv 1 \pmod{p^2}$ , so  $p | (m - 1)$ . But  $m$  is a multiple of  $p$ , so this is impossible.

Thus  $m$  is a product of distinct primes. Next suppose that  $2 | m$ . We can find an odd prime  $p$  dividing  $m$  as well (because 4 can't divide  $m$ , and  $m \neq 2$ ). Now let  $a$  be a primitive root mod  $p$ . Then the order of  $a \pmod{p}$ , which is  $p - 1$ , is even. But  $a^{m-1} \equiv 1 \pmod{p}$ , which is impossible because  $m - 1$  is odd.

Thus  $m$  is a product of distinct odd primes. Let  $p$  be one of those primes. Again, let  $a$  be a primitive root mod  $p$ . Then  $a^{m-1} \equiv 1 \pmod{p}$  implies that the order of  $a$ , which is  $p - 1$ , must divide  $m - 1$ . I think that's everything!

(c) This follows from Korselt's criterion, because  $(6k + 1)(12k + 1)(18k + 1) - 1 = 1296k^3 + 396k^2 + 36k$  is visibly divisible by  $6k$ ,  $12k$ , and  $18k$ .  $\square$

*Remark:* Note that on the problem set I remarked on a 1994 result showing there were infinitely many Carmichael numbers; this is only interesting if the definition of Carmichael number explicitly avoids prime numbers! I neglected to include that in the definition on the problem set.

**Problem 6:** This one's been put on the next problem set.

**Problem 7:** Show that there is an injective homomorphism  $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$  if and only if  $a|b$ .

**Solution:** First of all, the degree of the extension  $\mathbb{F}_{p^a}$  of  $\mathbb{F}_p$  is clearly  $a$ . And remember from algebra that degrees multiply in towers. In other words, if  $\mathbb{F}_{p^b}$  contains  $\mathbb{F}_{p^a}$ , then the degree of the big field over  $\mathbb{F}_p$  must be divisible by the degree of the smaller field over  $\mathbb{F}_p$ . So  $a|b$ .

As for the converse, suppose  $a|b$ . Then, as we have seen,  $x^{p^a} - x$  divides  $x^{p^b} - x$ . So it splits completely into linear factors in  $\mathbb{F}_{p^b}$ , because  $x^{p^b} - x$  does. And remember, the set of roots of  $x^{p^a} - x$  in a field  $F$  forms a subfield of  $F$  (that is, it contains 0 and 1, and it's closed under addition, multiplication, and inversion.) So it must be  $\mathbb{F}_{p^a}$ . So we've actually constructed  $\mathbb{F}_{p^a}$  inside  $\mathbb{F}_{p^b}$ . (This is not the only way to do the problem, but it's probably the most elementary.)  $\square$

**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

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

(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  $p$ .

**Solution:** (a) For every  $x \pmod p$ , we get  $y^2 \equiv -x^2 - 1$ , so there are at most two solutions  $y$  for every  $x$ . This gives the bound  $n_p \leq 2p$  in general (there are  $p$  choices for  $x$ ). Now note that if  $p \equiv 3 \pmod 4$ , if  $x = 0$  then  $y^2 \equiv -1 \pmod p$ , which has no solutions. So that gives the better bound  $n_p \leq 2(p - 1)$  in this case. Also note that if  $p \equiv 1 \pmod 4$ , then there are always at least two solutions  $(0, \pm\alpha)$ , where  $\alpha$  is a square root of  $-1 \pmod p$ . So that gives all the inequalities we want.

(b) Every solution  $(x_0, y_0)$  to the two-variable congruence extends to  $p - 1$  nontrivial solutions  $(\lambda x_0, \lambda y_0, \lambda)$  to the three-variable congruence, where  $\lambda \neq 0$ . Which solutions to the three-variable congruence are not generated in this way? Precisely the ones where  $z = 0$ . (Otherwise  $(x, y, z)$  is extended from  $(x/z, y/z)$ .) How many solutions with  $z = 0$  are there? Well, the resulting congruence is  $x^2 + y^2 \equiv 0 \pmod p$ . If  $y = 0$  we get  $x = 0$ , and otherwise we get  $x^2 \equiv -y^2 \pmod p$ , and this has a nontrivial solution if and only if  $-1$  is a square mod  $p$ , in which case there are two solutions  $y$  for every nonzero  $x$ . So if  $p \equiv 3 \pmod 4$  there is one extra solution, and if  $p \equiv 1 \pmod 4$  there are  $1 + 2(p - 1)$  extra solutions. This gives the equality in part (b).

(c) Consider the equalities in (b) mod  $p$ . We get  $n_p \equiv 1 \pmod p$  if  $p \equiv 3 \pmod 4$ , and  $n_p \equiv -1 \pmod p$  if  $p \equiv 1 \pmod 4$ . Coupled with the inequalities in part (a), we get that  $n_p = 1$  or  $p + 1$  if  $p \equiv 3 \pmod 4$ , and  $n_p = p - 1$  or  $2p - 1$  if  $p \equiv 1 \pmod 4$ . But we can decide which it is if we show that  $n_p$  must be even.

To see this, we realize that if  $(x, y)$  is a solution, then so is  $(x, -y)$ . This splits every solution into pairs, except for the ones with  $y = 0$ . But there are either 0 or 2 such solutions depending on whether  $p \equiv 3$  or  $1 \pmod 4$ , respectively. There you have it. Since  $n_p$  is even, we know what it must be in both cases.  $\square$