

**Problem Set 4 Due Apr. 15. 2008**

1. Section 22 (page 207) Problems 12-15.

SOLUTION: 12. Easy trial and error.  $1^2 + 1 = 0$ ,  $0^2 + 1 = 1 \neq 0$ , so 1 is the only root.

13. Brute force trial and error or trial and error to first root. 0, 1 are not roots by inspection.  $2^3 + 2 \cdot 2 + 2 = 1 + 4 + 2 = 7 = 0$ , so 2 is a root. Now factor.

$$\begin{array}{r|rrrr}
 x-2 & x^2 & +2x & +6 & \\
 & x^3 & +0x^2 & +2x & +2 \\
 & x^3 & -2x^2 & +0x & +0 \\
 \hline
 & & 2x^2 & +2x & +2 \\
 & & 2x^2 & -4x & 0 \\
 \hline
 & & & 6x & +2 \\
 & & & 6x & -12 \\
 \hline
 & & & & 14(=0)
 \end{array}$$

This factors as  $(x-2)(x-3)$ , noting that  $-5x = 2x$ . So 3 is also a root and there are no others. (Perhaps brute force is easiest here, but I'm trying to make a point. Note the double root.)

14. Substituting 0, 1, 2, -2, -1, respectively, the results are 0, 2, 4, 4, 0, respectively. So 0 and 4 are the only roots.

15. Since  $\mathbb{Z}_7$  is a field,  $a$  is a root of  $f(x)g(x)$  if and only if  $a$  is a root of  $f(x)$  or  $g(x)$ . 0 is obviously a root of  $g(x)$ , and any other root must satisfy  $3a + 2 = 0$ , so  $a = 3^{-1}(-2) = 5(-2) = -10 = 4$  is also a root. This leaves 1, 2, 3, -2, -1 as candidate roots of  $f(x)$ . These give 1, 0, 5, 1, 1, respectively, so 0, 2, 4 are the only roots.

2. Section 22 (page 207) Either 16 or 17.

SOLUTION: 16.  $\varphi_3(x^{231} + 3x^{117} - 2x^{53} + 1) = 3^{231} + 3 \cdot 3^{117} - 2 \cdot 3^{53} + 1$ . Noting that  $231 \equiv 3$ ,  $117 \equiv 1$ ,  $53 \equiv 1$ , ( $\pmod{4}$ ), the computation simplifies to  $3^3 + 3^2 - 2 \cdot 3 + 1 = 2 + 4 - 6 + 1 = 1$ ,  $\pmod{5}$ . Note my use of  $\pmod{p-1}$  for powers, where  $p$  is, in this case, the prime number 5.

17. Note that 219, 74, 57, 44 are congruent to -1, 2, 1, 0 ( $\pmod{4}$ ), respectively. 0 is clearly a root. For 1, we compute  $2 + 3 + 2 + 3 = 0$ , so 1 is a root. Trying 2 (its inverse is 3), we compute  $2 \times 3 + 12 + 4 + 3 = 0$ ,

Trying  $-2$  (its inverse is  $2$ ), we compute  $-6 + 2 - 4 + 3 = -5 = 0$ , so  $3$  is also a root. Trying  $-1$ , we compute  $-2 + 3 - 2 + 3 = 2 \neq 0$ , so  $4$  is not a root.

3. Section 22 (page 208) Problem 22 and extra problem. In  $\mathbb{Z}^\infty[x]$  (power series with integer coefficients) I showed in class that  $\sum_{i=0}^\infty a_i x^i$  is a unit if and only if  $a_0 = 1$ . Compute the inverse of  $1 + 2x$  as a power series. This computation is still valid in  $\mathbb{Z}_n^\infty[x]$ . Now show that  $1 + 2x$  has an inverse in  $\mathbb{Z}_{2^n}[x]$ , and compute it for  $n = 1$  and  $n = 4$ .

The inverse power series for  $1 + 2x$  is  $\sum_{i=0}^\infty (-2)^i x^i$ . In  $\mathbb{Z}_{2^n}[x]$ ,  $2^i = 2^{-i} = 0$  for  $i \geq n$ . That is, the infinite power series becomes finite, with just  $n$  non-zero terms, so it is a polynomial. For  $n = 1$ ,  $1 + 2x = 1$ , so the inverse is trivial;  $1$ . For  $n = 4$ , the inverse is  $1 - 2x + 4x^2 - 8x^3$ . To solve the problem in the text, take  $n = 2$  to obtain  $1 - 2x = 1 + 2x$  as the inverse of itself. For  $n = 4$ , direct computation confirms the answer as follows:  $(1 + 2x)(1 - 2x + 4x^2 - 8x^3) = 1 - 2x + 4x^2 - 8x^3 + 2x - 4x^2 + 8x^3 - 16x^4 = 1 - 16x^4 = 1$ .

4. Section 23 (page 218) Divide  $g(x)$  into  $f(x)$  to obtain a remainder polynomial. Choose any two of problems 1-4.

SOLUTION: Results. 1.  $q(x) = x^4 + x^3 + x^2 + x - 2$  and  $r(x) = 4x + 3$ .  
2.  $q(x) = 5x^4 + 5x^2 - x$  and  $r(x) = x + 2$ .  
3.  $q(x) = 6x^4 + 7x^3 + 2x^2 - x + 2$  and  $r(x) = 4$ .  
4.  $q(x) = 9x^2 + 5x + 10$  and  $r(x) = 2$ .

5. Section 23 (page 218) 7 and 8. Make sure you remind yourself of Corollary 6.16.

SOLUTION: 7. In  $\mathbb{Z}_{17}$ ,  $\langle 2 \rangle = \{2, 4, 8, 16\}$ . Trying  $3$ , we observe that  $3^1 = 3, 3^2 = 9, 3^3 = 10, 3^4 = 13, 3^5 = 5, 3^6 = 15 = -2, 3^7 = -6 = 11, 3^8 = 33 = 16 = -1$ . We can stop here, since  $3^{8+i} = -3^i$ . The next 8 numbers will all be different, ending with  $-(-1) = 1$ . Thus,  $3$  generates the multiplicative group of non-zero integers, mod 17. All generators are given by  $3^n$ , where  $\gcd(n, 16) = 1$ . In this case,  $n$  is odd. The generators are  $3, 3^3 = 10, 3^5 = 5, 3^7 = 11, 3^9 = -3 = 14, 3^{11} = -10 = 7, 3^{13} = -5 = 12, 3^{15} = 6$ .

8.  $23 - 1 = 22 = 2 \times 11$ . Starting with 2, we compute  $2^1 = 2, 2^2 = 4$ . At this point, we know that  $|\langle 2 \rangle| \neq 2$ , so it is either 11 or 22.  $2^{11} = 2048 = 89 \times 23 + 1 = 1$ . Thus, 2 does not generate the group. However, our computations show that  $(-2)^{11} = -1$ , so that  $-2 = 21$  must be a generator. All the generators are given by  $(-2)^n$ , where  $\gcd(n, 22) = 1$ . This means all odd numbers  $< 23$ , except for 11. The generators are  $(-2)^1 = 21, (-2)^3 = -8 = 15, (-2)^5 = -32 = -9 = 14, (-2)^7 = -36 = 10, (-2)^9 = 6, (-2)^{13} = -4 = 19, (-2)^{15} = -16 = 7, (-2)^{17} = 28 = 5, (-2)^{19} = 20, (-2)^{21} = -12 = 11$ . The smallest positive generator is 5.

6. Section 23 (page 218) Problems 11 and 17.

SOLUTION: 11. We are told that the polynomial has three roots. By inspection (after 0, 1, 2 all fail), 3 is a root. Divide to obtain  $2(x - 3)(x^2 - x - 1)$ . By inspection, the quadratic has roots  $-3$  and 4, so the factorization is  $(x - 3)(x + 3)(2x - 8)$ .

17. If  $p(x) = x^4 - 22x^2 + 1$  is reducible over  $\mathbb{Q}$  if and only if it is reducible over  $\mathbb{Z}$ . If  $p(x)$  had a linear factor, the constant term in  $p(x)$  shows that the linear term could only be  $(x \pm 1)$ . This is false, since neither 1 nor  $-1$  are roots of  $p(x)$ . Any factorization would be of the form  $(x^2 + ax + b)(x^2 + cx + d)$ . Clearly  $b = d = \pm 1$ . The  $x^3$  coefficient is 0, so  $a + c = 0$ . The  $x^2$  coefficient is  $-22$ , so  $-22 = ac + b + d$ . Finally the  $x$  coefficient is 0, so  $bc + ad = 0$ . Eliminating both  $c = -a$  and  $d = b$ , we obtain  $-22 = -a^2 + 2b$ .  $b = -1$  forces  $a = c$ , so  $a = c = -c = 0$ , which is impossible. With  $b = d = 1$ , we get  $-22 = a^2 + 2$ , equivalent to  $a^2 + 24 = 0$ , which is impossible as well. Therefore,  $p(x)$  is irreducible.

7. Section 23 (page 219) Problems 18-21. (Easy with the Eisenstein criterion.)

SOLUTION: 18. Yes.  $p = 3$

19. Yes.  $p = 3$

20. No. The only possible prime is 2, which does not divide the coefficient 9.

21. Yes.  $p = 5$ .

8. Section 23 (page 219) Problem 25 (True or False questions)

SOLUTION: In the given order: T T T F T T T T T T Note that e. and f. are identical questions. What gives? I should contact the author.

9. Section 23 (page 219) Problem 34. (This type of question could be on an exam.)

SOLUTION: I'll show that  $x^p + a$  is reducible by finding a root. If  $b$  is any non-zero element of  $\mathbb{Z}_p$ , then  $b^p = b \cdot b^{p-1} = b \cdot 1 = b$ . Thus,  $-a = (p - a)$  is a root of the equation.

10. If  $p > 3$  is a prime number, prove that the polynomial,  $\left[ \prod_{i=1}^{p-2} (i + x) \right] + 1$ , is not irreducible in  $\mathbb{Z}_p$ .

SOLUTION: For  $x = 1$ , the product is  $(p - 1)! = -1$ , so 1 is a root of the polynomial. It has a linear factor, so it is not irreducible.

11. Following the usual convention, let  $\mathbb{H}^*$  be the set of non-zero quaternions. Then  $\mathbb{H}^*$  is a group under quaternion multiplication. Compute  $Z(\mathbb{H}^*)$ , the center of  $\mathbb{H}^*$ .
12. If  $a + bi + cj + dk$  commutes with every quaternion, it must commute with  $i$ ,  $j$  and  $k$ . Then

$$\begin{aligned} i(a + bi + cj + dk) &= -b + ai - dj + ck \\ \text{and} \\ (a + bi + cj + dk)i &= -b + ai + dj - ck, \end{aligned}$$

so  $c = d = 0$ . We must also have  $j(a + bi) = (a + bi)j$ , which implies that  $-bk = bk$ , so  $b = 0$  as well. Clearly any real number commutes with any quaternion, so  $Z(\mathbb{H}^*) = \mathbb{R}$ .