

85 minutes, 8 problems (both sides of sheet)

1. PROBLEM 1 (10 PTS)

For a positive integer  $n$ , let its usual decimal expansion be

$$n = \sum_{j=0}^k a_j 10^j$$

where the  $a_j$  are integers in the range  $0 \leq a_j \leq 9$ . Since  $10^j \equiv 1 \pmod{3}$  for all  $j \geq 0$ , we get the well-known rule generalizing the criterion for division by 3,

$$n \equiv \sum_{j=0}^k a_j \pmod{3},$$

and a little thought shows this also holds if 3 is replaced by 9.

In terms of the  $a_j$ , what are  $n \pmod{11}$  and  $n \pmod{7}$ ? (Provide formulas and prove them.)

*Solution:* Since  $10 \equiv -1 \pmod{11}$ ,

$$n \equiv \sum_{j=0}^k (-1)^j a_j \pmod{11}.$$

Similarly,  $10 \equiv 3 \pmod{7}$ , so

$$n \equiv \sum_{j=0}^k 3^j a_j \pmod{7}.$$

However, for full credit another step is needed. The numbers  $3^j$  grow large as ordinary integers, but  $3^6 \equiv 1 \pmod{7}$ , so

$$n = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 + \dots,$$

where the coefficients of the  $a_j$  are periodic with period 6.

2. PROBLEM 2 (15 PTS)

Find an integer  $n$  that solves  $n \equiv 51 \pmod{59}$ ,  $n \equiv 59 \pmod{151}$ .

*Solution:* The Euclidean algorithm run forward and backward gives (skipping the various steps that are involved)

$$1 = -25 \times 151 + 64 \times 59,$$

so  $n = -51 \times (25 \times 151) + 59 \times (64 \times 59) = 30259$  works, but for full credit this should be reduced  $\pmod{59 \times 151}$ , which gives  $n = 3532$ .

3. PROBLEM 3 (10 PTS)

What is  $\phi(119)$ , the Euler function of 119?

Find the number of solutions to

$$x^4 \equiv 2 \pmod{119}.$$

Exhibiting all the solutions  $\pmod{119}$  and showing they are the only ones is a hard way to do this. You are only asked to find the number of solutions.

*Solution:*  $119 = 7 \times 17$ , so  $\phi(119) = \phi(7)\phi(17) = 6 \times 16 = 96$ .

By the Chinese Remainder Theorem, the number of solutions mod 119 is the product of the number of solutions mod 7 and mod 17. Now there are 2 solutions mod 7, but none mod 17 (either by direct case-by-case verification, or by noticing that a potential solution would have  $x^{16} = 2^4 = -1 \pmod{17}$ , violating Fermat's Little Theorem), so the answer is zero.

4. PROBLEM 4 (10 PTS)

Are there any solutions over the integers to the equation

$$x^2 + 2xy + 8y^2 - 49z^3 = 3 ?$$

*Solution:* If we consider this equation mod 7, then the term with the variable  $z$  vanishes, and we are left with

$$x^2 + 2xy + y^2 = (x + y)^2 = 3 \pmod{7},$$

but  $u^2 = 3 \pmod{7}$  does not have a solution, so there is no solution to the original equation.

5. PROBLEM 5 (20 PTS)

Show that the polynomials  $f(x) = x^5 + x + 1$  and  $g(x) = x^3 + x^2 + 1$  are relatively prime in  $F_2[x]$ , and find a solution over  $F_2[x]$  to the simultaneous congruence

$$h(x) = x^4 + x \pmod{f(x)},$$

$$h(x) = x + 1 \pmod{g(x)}.$$

*Solution:* This was a very unfortunate typo on my part.  $f(x)$  was supposed to be  $x^5 + x^2 + 1$ , in order to be similar to what's in the book, but slightly different. (We have encountered these polynomials before, in the context of CRCs, and saw that for the  $f(x)$  and  $g(x)$  given on the exam,  $g(x)$  divides  $f(x)$ .)

Grading on this problem and the next one was very lenient, as long as something sensible and correct was done, credit was given. But for the corrected problem, with  $f(x) = x^5 + x^2 + 1$  and  $g(x) = x^3 + x^2 + 1$ , running the Euclidean algorithm gives

$$1 = x \times f(x) + (x^3 + x^2 + x + 1) \times g(x),$$

and the desired  $h(x) = x^5 + x^4 + x^2 + x + 1$ . (The basic Euclidean algorithm procedure produces a higher degree polynomial, this one has been reduced modulo the product of  $f(x)$  and  $g(x)$ .)

6. PROBLEM 6 (10 PTS)

Let  $f(x)$  and  $g(x)$  be as in the problem above, and let  $f^*(x) = (x + 1)f(x)$  and  $g^*(x) = (x + 1)g(x)$ , all in  $F_2[x]$ . Find a solution over  $F_2[x]$  to

$$h(x) = x + 1 \pmod{f^*(x)},$$

$$h(x) = x^4 + x \pmod{g^*(x)}.$$

*Solution:* Whatever the  $f(x)$  and  $g(x)$  are, provided they are relatively prime to each other, and each is relatively prime to  $x + 1$ , let  $H(x)$  be the solution to

$$H(x) = x + 1 \pmod{f(x)},$$

$$H(x) = x^4 + x \pmod{g(x)}.$$

(This solution can be obtained from the intermediate results, those coming from the Euclidean algorithm, for the previous problem, if  $f(x)$  and  $g(x)$  are as in the corrected version of that problem.)

Then notice that the desired  $h(x)$  comes from solving

$$\begin{aligned}h(x) &= H(x) \bmod f(x)g(x), \\h(x) &= 0 \bmod (x+1)\end{aligned}$$

and this is either  $H(x)$  or  $H(x) + f(x)g(x)$ .

The point of this problem was to show that one can use the Chinese Remainder Theorem even in cases where the moduli are not prime, by small tweaks.

#### 7. PROBLEM 7 (15 PTS)

What are the irreducible monic (i.e., leading coefficient 1) polynomials of degree 2 over  $F_3$ ?

How many irreducible monic polynomials of degree 3 over  $F_3$  are there? (Finding them all is not required, and is the hard way to solve this problem.)

*Solution:* All these polynomials have to be of the form  $x^2 + ax + b$ , where  $a, b = 0, 1, 2$  and cannot vanish when  $x$  takes on the values 0, 1, 2. Non-vanishing at  $x = 0$  means  $b = 1, 2$ , and testing the remaining 6 cases shows that the irreducibles are

- $x^2 + 1$
- $x^2 + x - 1$
- $x^2 - x - 1$

(There are some shortcuts one can make, such as noticing that  $f(x)$  is irreducible if and only if  $f(x)$  is, so that cuts down the number of cases to be tried, in that can take  $a = 0, 1$ .)

For cubics, there are  $27 = 3^3$  monic ones in all (as we get to choose coefficients of the constant, linear, and quadratic terms at will). The reducible ones arise as products of a monic linear term and a monic irreducible quadratic ( $3 \times 3 = 9$  ways) or else as a product of 3 linear monic polynomials (repetitions allowed), which can happen in 10 ways, either product of all three linear monic polynomials (1 way), or a cube of a linear monic (3 ways), or square of a linear monic (3 ways to choose it) times a distinct linear monic (2 remaining ones to choose from). So we get 19 reducible monic cubics, and that leaves 8 irreducible ones.

#### 8. PROBLEM 8 (10 PTS)

Let  $F_9$  be defined as  $F_3[x]/(x^2 + 1)$ , and let  $\alpha$  be the image of  $x$ . What is the multiplicative inverse of  $\alpha$ ?

Compute  $\alpha^{20090325}$  in  $F_9$ .

*Solution:* There are not many choices, and it's probably simplest to just test them, and see that  $x \times (-x) = 1 \bmod (x^2 + 1)$ , so  $-\alpha = 2\alpha$  is the multiplicative inverse of  $\alpha$ .

Since  $\alpha^4 = 1$ ,  $\alpha^{20090325} = \alpha^{4 \times 5022581 + 1} = (\alpha^4)^{5022581} \times \alpha = \alpha$ .