

**MATH 465 NUMBER THEORY, SPRING TERM  
2009, PRACTICE EXAM 2, MODEL SOLUTIONS**

1. (25 marks) Solve the simultaneous congruences  $x \equiv 4 \pmod{19}$ ,  $x \equiv 5 \pmod{31}$ . Solve  $31a \equiv 1 \pmod{19}$  and  $19b \equiv 1 \pmod{31}$ . By Euclid's algorithm,  $1 = 8 \cdot 31 - 13 \cdot 19$ , Thus  $a = 8$ ,  $b \equiv -13 \equiv 18 \pmod{31}$ .  $19 \cdot 31 = 589$ . Hence  $x \equiv 4 \cdot 8 \cdot 31 + 5 \cdot 18 \cdot 19 \equiv 346 \pmod{589}$

2. (25 marks) Find all solutions to the congruence  $x^{38} + 12x^{20} + 6x \equiv 0 \pmod{19}$ . By Fermat's Little Theorem,  $x^{19} \equiv x \pmod{19}$ , so  $x^{38} \equiv x^2 \pmod{19}$  and  $x^{20} \equiv x^2 \pmod{19}$ . Thus  $x^{38} + 12x^{20} + 6x \equiv 13x^2 + 6x \equiv 13(x^2 - x) \pmod{19}$ . Hence  $x \equiv 1$  or  $x \equiv 0 \pmod{19}$ .

3. (25 marks) (i) Solve  $x^2 + x + 23 \equiv 0 \pmod{5}$ . Let  $f(x) = x^2 + x + 23$ . Then  $f(0) = 23$ ,  $f(1) = 25$ ,  $f(2) = 26$ ,  $f(3) = 35$ ,  $f(4) = 43$ . Hence  $x_0 = 1$  or  $3$ .

(ii) Use the Hensel-Newton method to find all solutions to  $x^2 + x + 23 \equiv 0 \pmod{5^2}$ . Note that  $f'(1) = 3 \not\equiv 0 \pmod{5}$ ,  $f'(3) = 7 \equiv 2 \not\equiv 0 \pmod{5}$ .  $x_0 = 1$ . Then  $f'(1)^{-1} \equiv 2 \pmod{5}$ ,  $x_1 = 1 - f(1)f'(1)^{-1} \equiv 1 \pmod{5^2}$ .  $x_0 = 3$ . Then  $x_1 = 3 - f(3)f'(3)^{-1} \equiv 3 - 35 \cdot 3 \pmod{5^2} \equiv 23 \pmod{5^2}$ . Thus  $x_1 = 1$  or  $23$ .

4. (25 marks) Show that 2 is a primitive root modulo 11 and draw up a table of indices to this base modulo 11. Hence, or otherwise, find all solutions to the following congruences, (i)  $x^6 \equiv 7 \pmod{11}$ , (ii)  $x^{48} \equiv 9 \pmod{11}$ , (iii)  $x^7 \equiv 8 \pmod{11}$ .

$y$	1	2	3	4	5	6	7	8	9	10
$2^y$	2	4	8	5	10	9	7	3	6	1

---

$x$	1	2	3	4	5	6	7	8	9	10
$\text{ind}_2 x$	10	1	8	2	4	9	7	3	6	5

(i) This is equivalent to  $6y \equiv 7 \pmod{10}$ . Since  $(6, 10) = 2 \nmid 7$  there is no solution. (ii)  $48y \equiv 6 \pmod{10}$ ,  $24y \equiv 3 \pmod{5}$   $1 \leq y \leq 10$ ,  $y \equiv 2 \pmod{5}$ ,  $y \equiv 2$  or  $7 \pmod{10}$ ,  $x \equiv 4$  or  $7 \pmod{11}$  (iii)  $7y \equiv 3 \pmod{10}$ ,  $y \equiv 9 \pmod{10}$ ,  $x \equiv 6 \pmod{11}$ .