

INTRODUCTION TO NUMBER THEORY

Exam 3

April 27, 2007

The point value of each problem is given in the margin.

(8) 1. Find the least complete solution of the congruence, (that is all solutions mod 21).

$$6x \equiv 27 \pmod{21}.$$

$$\Leftrightarrow 2x \equiv 9 \pmod{7}$$

$$\Leftrightarrow 4 \cdot 2x \equiv 4 \cdot 9 \pmod{7}$$

$$\Leftrightarrow x \equiv 36 \equiv 1 \pmod{7}$$

$$\Leftrightarrow x \equiv 1, 8, 15 \pmod{21}$$

2. Short answer.

(3) a) If $f(x)$ is a polynomial of degree 5 what is the greatest number of solutions the congruence $f(x) \equiv 0 \pmod{7}$ can have? 5, by Lagrange's Theorem
(Assume $f(x)$ is not identically zero $\pmod{5}$.)

What is the greatest number of solutions $f(x) \equiv 0 \pmod{35}$ can have? 25, since $f(x) \equiv 0 \pmod{5}$ can have 5 solutions and $f(x) \equiv 0 \pmod{7}$ can have 5 solutions.

(3) b) If $f(x)$ is a polynomial of degree d and p is a prime such that the congruence $f(x) \equiv 0 \pmod{p}$ has 2 distinct solutions \pmod{p} , one singular, one nonsingular, how many solutions can the congruence $f(x) \equiv 0 \pmod{p^2}$ have? (Give all possibilities.)

1 if the singular solution does not lift.

$p+1$ if the singular solution does lift.

(3) c) What are the possible values for the order of $a \pmod{23}$, if $23 \nmid a$? $\text{ord}_{23}(a) \mid 22$

Thus $\text{ord}_{23}(a) = 1, 2, 11$ or 22

(3) d) If m is an odd number such that $2^{m-1} \equiv 1 \pmod{m}$ but $2^{\frac{m-1}{2}} \equiv 2 \pmod{m}$ can we make any conclusion as to whether m is a prime or not? Explain.

m must be composite, because if m was a prime then $2^{\frac{m-1}{2}} \equiv \pm 1 \pmod{m}$.

$$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

(10) 7. (State) and prove Euler's Theorem (on raising numbers to a power \pmod{m} .)

Let $\{a_1, a_2, \dots, a_{\phi(m)}\}$ be a reduced residue system \pmod{m} .

Since $(a, m) = 1$, we know $\{aa_1, aa_2, \dots, aa_{\phi(m)}\}$ is also a reduced res. system \pmod{m} . Thus

$$a \cdot a_2 \cdots a_{\phi(m)} \equiv (aa_1)(aa_2) \cdots (aa_{\phi(m)}) \pmod{m}$$

$$\Rightarrow a \cdot a_2 \cdots a_{\phi(m)} \equiv a^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} \pmod{m}$$

$$\Rightarrow 1 \equiv a^{\phi(m)} \pmod{m}, \text{ by cancellation (since } (a_i, m) = 1 \text{ for all } i.)$$

(10) 8. In the RSA method of public cryptography suppose that you have chosen $p = 5$, $q = 13$, $e = 5$, $m = pq = 65$.

a) Calculate the decode exponent d . Recall, d is the multiplicative inverse of e modulo the least common multiple $[p-1, q-1]$.

$$[p-1, q-1] = [4, 12] = 12, \quad e = 5, \text{ so we must solve } 5x \equiv 1 \pmod{12}.$$

By trial & error we get $x \equiv 5 \pmod{12}$ works and so $d = 5$.

(or you can solve $5x + 12y = 1$ using array method

$5x + 12y$	5	12	2	1
x	1	0	-2	5
y	0	1	1	-2

b) Suppose that we start with a message M_0 (expressed as a number) with $0 < M_0 < m$, $(M_0, m) = 1$. Explain how to encode the message and then how to decode the message.

$$M_1 = \text{encoded message}, \quad M_1 \equiv M_0^e \pmod{m}, \quad 0 < M_1 < m.$$

$$M_2 = \text{decoded message}, \quad M_2 \equiv M_1^d \pmod{m}, \quad 0 < M_2 < m.$$

$$\text{It follows that } M_2 \equiv M_0 \pmod{m}$$

c) What is it that allows the RSA method to be secure and yet public?

It is secure because the primes p, q are chosen to be extremely large (over 100 digits) so that it becomes impossible (from a computational view) to factor m . Thus the modulus m can be made public and e can be made public, but the public cannot determine d , since they do not know p & q .

- (10) 3. In order to count the number of pennies in a large jar they are first stacked into groups of 5, with 1 left over. Next, they are stacked into groups of 6, with 2 left over. Finally, they are stacked into groups of 7 and none are left over. It is known that there are between 200 and 400 pennies in the jar. How many are there?

Let $x = \#$ pennies in the jar

$$\text{CRT} \begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 2 \pmod{6} \\ x \equiv 0 \pmod{7} \end{cases} \rightarrow x = 7s \text{ for some integer } s.$$

$$7s \equiv 2 \pmod{6} \Rightarrow s \equiv 2 \pmod{6} \Rightarrow s = 2 + 6t, \quad t \in \mathbb{Z} \\ \Rightarrow x = 14 + 42t$$

$$14 + 42t \equiv 1 \pmod{5} \\ 2t \equiv -2 \pmod{5}, \text{ since } (2, 5) = 1, \text{ it can be cancelled.} \\ t \equiv 1 \pmod{5}$$

$$x \equiv 14 + 42 \pmod{210}, \quad x \equiv 56 \pmod{210}.$$

Since $200 < x < 400$ we must have $x = 56 + 210 = 266$

- (10) 4. Say the decimal expansion of $66/325$ is given by

$$\frac{66}{325} = .a_1 a_2 \dots a_i \overline{c_1 c_2 \dots c_k}$$

with i, k minimal. Find the values of i, k . (Use the theory to obtain i, k . You can check your answer by long division or on your calculator.)

$$66 = 2 \cdot 3 \cdot 11 \\ 325 = 25 \cdot 13 = 5^2 \cdot 13 \quad \left. \vphantom{\begin{matrix} 66 \\ 325 \end{matrix}} \right\} \text{Note } (66, 325) = 1.$$

$$325 \mid 10^i (10^k - 1) \Leftrightarrow 5^2 \mid 10^i \text{ and } 13 \mid 10^k - 1$$

$$\Leftrightarrow i \geq 2 \quad \text{and} \quad 10^k \equiv 1 \pmod{13}.$$

By FLT $10^{12} \equiv 1 \pmod{13}$. We must test divisors of 12.

$$10^1 \equiv -3 \pmod{13}$$

$$10^2 \equiv 9 \pmod{13}$$

$$10^3 \equiv -27 \equiv -1 \pmod{13}$$

$$10^4 \equiv (-4)^2 \equiv 3 \pmod{13}$$

$$10^6 \equiv (-1)^2 \equiv 1 \pmod{13}$$

Thus $\text{ord}_{13}(10) = 6$ and we get $i = 2, k = 6$.

(10) 5. If $(a, m) = 1$, $k = \text{ord}_m(a)$ and $a^n \equiv 1 \pmod{m}$, prove that $k|n$.

By division alg. $n = qk + r$ for some q, r with $0 \leq r < k$.

$$\text{Then } a^n \equiv 1 \pmod{m} \Rightarrow a^{qk+r} \equiv 1 \pmod{m}$$

$$\Rightarrow (a^k)^q a^r \equiv 1 \pmod{m}$$

$$\Rightarrow 1^q \cdot a^r \equiv 1 \pmod{m}$$

$$\Rightarrow a^r \equiv 1 \pmod{m}$$

Since $r < k$, it follows that $r = 0$ (since k is the minimal exponent with $a^k \equiv 1 \pmod{m}$).

Thus $n = qk$, that is, $k|n$.

(10) 6. Use the method of lifting solutions to find all solutions of the congruence

$$x^3 \equiv 7 \pmod{25}.$$

$$\text{Start (mod 5): } x^3 \equiv 7 \pmod{5} \Leftrightarrow x^3 \equiv 2 \pmod{5}$$

Testing 0, 1, 2, 3, -1, we see that there is only one solution $x \equiv 3 \pmod{5}$.

$$\text{Lift to (mod 25): } x = 3 + 5t.$$

$$\text{Lifting congruence, } f'(a)t \equiv -\frac{f(a)}{5} \pmod{5}$$

$$f(x) = x^3 - 7, a = 3$$

$$27t \equiv -\frac{20}{5} \pmod{5}$$

$$f(3) = 20$$

$$2t \equiv 1 \pmod{5}$$

$$f'(x) = 3x^2$$

$$t \equiv 3 \pmod{5}$$

$$f'(3) = 27$$

$$x \equiv 3 + 5 \cdot 3 \pmod{25}$$

$$x \equiv 18 \pmod{25}$$