

MA4016 - Engineering Mathematics 6

Solution Sheet 7: Number Theory (March 19, 2010)

1. Find 11^{644} mod 645 and 123^{1001} mod 101 using fast modular exponentiation. We have 644=512+128+4 and 1001=512+256+128+64+32+8+1, and compute

Thus

$$11^{644} \mod 645 = 226 \cdot 121 \cdot 451 \mod 645 = 256 \cdot 451 \mod 645 = 1$$

and

$$123^{1001} \mod 101 = \underbrace{52 \cdot 31}_{97 \cdot 92} \cdot \underbrace{58 \cdot 19}_{97 \cdot 92} \cdot \underbrace{25 \cdot 56}_{92} \cdot 22 \mod 101$$
$$= \underbrace{97 \cdot 92}_{96 \mod 101} \cdot \underbrace{87 \cdot 22}_{96 \mod 101} \mod 101 = 22.$$

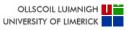
2. Solve the congruence $2x \equiv 7 \mod 17$. It holds $17 = 2 \cdot 8 + 1$ and therefore

$$-8 \cdot 2 \equiv 9 \cdot 2 \equiv 1 \mod 17$$
.

Thus 9 is an inverse of 2 modulo 17. We multiply the congruence with 9 and get

$$2x \equiv 7 \mod 17 \Leftrightarrow 9 \cdot 2x \equiv 9 \cdot 7 \equiv 12 \mod 17 \Leftrightarrow x \equiv 9 \cdot 7 \equiv 12 \mod 17.$$

University of Limerick Department of Mathematics and Statistics Dr. S. Franz



3. Find all solutions to the system of congruences.

$$x \equiv 2 \pmod{3}$$
, $x \equiv 1 \pmod{4}$, $x \equiv 3 \pmod{5}$.

The set $\{3,4,5\}$ is pairwise relatively prime and we can apply the Chinese Remainder Theorem. Thus $m=3\cdot 4\cdot 5=60$ and

$$M_1 = 60/3 = 20$$
, $20y_1 \mod 3 = 2y_1 \mod 3 \stackrel{!}{=} 1$ $\Rightarrow y_1 = 2$
 $M_2 = 60/4 = 15$, $15y_2 \mod 4 = 3y_2 \mod 4 \stackrel{!}{=} 1$ $\Rightarrow y_2 = 3$
 $M_3 = 60/5 = 12$, $12y_3 \mod 5 = 2y_3 \mod 5 \stackrel{!}{=} 1$ $\Rightarrow y_3 = 3$.

We get $x \equiv 2 \cdot 2 \cdot 20 + 1 \cdot 3 \cdot 15 + 3 \cdot 3 \cdot 12 \equiv 80 + 45 + 108 \equiv 20 + 45 + 48 \equiv 54 \pmod{60}$.

4. Find all solutions, if any, to the system of congruences.

$$x \equiv 5 \pmod{6}$$
, $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$.

The set $\{6, 10, 15\}$ is not pairwise relatively prime and therefore the Chinese Remainder Theorem cannot be applied directly. But we can transform the system of congruences into another more suitable one. We have

$$x \equiv 5 \pmod{6}$$
 $\Leftrightarrow x \equiv 1 \pmod{2}$ $x \equiv 2 \pmod{3}$ $\Rightarrow x \equiv 3 \pmod{10}$ $\Leftrightarrow x \equiv 1 \pmod{2}$ $\Rightarrow x \equiv 3 \pmod{5}$ $\Rightarrow x \equiv 3 \pmod{5}$ $\Rightarrow x \equiv 3 \pmod{5}$ $\Rightarrow x \equiv 3 \pmod{5}$

This new system has 6 congruences with redundancies—here the compact version

$$x \equiv 1 \pmod{2}$$
, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$.

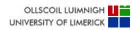
Now we can apply the Chinese Remainder Theorem and have $m=30,\ M_1=15,\ M_2=10,\ M_3=6$ and $y_1=y_2=y_3=1.$ The solution is

$$x \equiv 15 + 20 + 18 \equiv 53 \equiv 23 \pmod{30}$$
.

An alternative way is to start with $x = 6k_1 + 5 = 10k_2 + 3 = 15k_3 + 8$ with integers k_1, k_2, k_3 . By elimination we end with

$$k_1 = 5k + 3$$
, $k_2 = 3k + 2$, $k_3 = 2k + 1$ with any integer k

and get finally x = 30k + 23—the same solution as above.



5. a) Use Fermat's Little Theorem to compute $3^{302} \mod 5$, $3^{302} \mod 7$, and $3^{302} \mod 11$.

FLT gives

$$3^4 \mod 5 = 1$$
. $3^6 \mod 7 = 1$. $3^{10} \mod 11 = 1$.

and
$$302 = 4 \cdot 75 + 2 = 6 \cdot 50 + 2 = 10 \cdot 30 + 2$$
. Thus

$$3^{302} \equiv 3^2 \cdot (3^4)^{75} \equiv 9 \equiv 4 \pmod{5},$$

$$3^{302} \equiv 3^2 \cdot (3^6)^{50} \equiv 9 \equiv 2 \pmod{7},$$

$$3^{302} \equiv 3^2 \cdot (3^{10})^{30} \equiv 9 \pmod{11}$$
.

b) Use the results from part a) and the Chinese Remainder Theorem to find 3^{302} mod 385. Note that $305 = 5 \cdot 7 \cdot 11$.

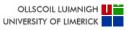
 $x = 3^{302} \mod 385$ is congruent to the system

$$x \equiv 4 \pmod{5}, \quad x \equiv 2 \pmod{7}, \quad x \equiv 9 \pmod{11}.$$

We apply CRT and compute $m=385,\ M_1=77,\ M_2=55,\ M_3=35,\ y_1=3,\ y_2=6$ and $y_3=6.$ We obtain

$$x \equiv 4.3.77 + 2.6.55 + 9.6.35 \equiv 924 + 660 + 1890 \equiv 154 + 275 + 350 \equiv 779 \equiv 9 \pmod{385}$$
.

University of Limerick Department of Mathematics and Statistics Dr. S. Franz



6. Suppose that we choose for the RSA-cryptosystem the primes p=17 and q=23, and the encryption exponent e=31. Compute n, $\varphi(n)$ and d. Encrypt 101 and decrypt 250 using above parameters.

 $n=p\cdot q=391$ and $\varphi(n)=(p-1)(q-1)=352.$ The inverse of e modulo 351 can be found using the extended Euclidean algorithm.

$$352 = 31 \cdot 11 + 11$$
 $11 = 351 - 31 \cdot 11$
 $31 = 11 \cdot 2 + 9$ $9 = 31 - 11 \cdot 2$
 $11 = 9 \cdot 1 + 2$ $2 = 11 - 9 \cdot 2$
 $9 = 2 \cdot 4 + 1$ $1 = 9 - 2 \cdot 4$
 $2 = 1 \cdot 2 + 0$

Thus
$$1 = 9 - 2 \cdot 4 = 9 \cdot 5 - 11 \cdot 4 = 31 \cdot 5 - 11 \cdot 14 = 159 \cdot 31 - 14 \cdot 352$$
 and

$$159 \cdot 31 \equiv 1 \pmod{352} \quad \Rightarrow d = 159.$$

Encrypting 101: For encrypting we assume only to know e=31 and n=391. Therefore we use the fast modular exponentiation to compute $C=101^{31}$ mod 391. We have

$$101^{1} \mod 391 = 101$$

 $101^{2} \mod 391 = 35$
 $101^{4} \mod 391 = 35^{2} \mod 391 = 52$
 $101^{8} \mod 391 = 52^{2} \mod 391 = 358$
 $101^{16} \mod 391 = 358^{2} \mod 391 = 307$

and $C=109\cdot 35\cdot 52\cdot 358\cdot 307$ mod 391 = 186. For decryption we know p=17, q=23 too. We will apply FLT and CRT we reduce computational costs. We rewrite 250^{159} mod 391 into a congruent system using FLT

$$250^{159} \mod 17 = 12^{159} \mod 17 = 12^{15} (12^{16})^9 \mod 17 = 12^{15} \mod 17 = 10$$

 $250^{159} \mod 23 = 20^{159} \mod 23 = 20^5 (20^{22})^7 \mod 23 = 20^5 \mod 23 = 10$

and fast modular exponentiation for the final steps. We now solve the system

$$D \equiv 10 \pmod{17}$$
, $D \equiv 10 \pmod{23}$.

In this special case we don't need CRT and we can conclude directly

$$17|(D-10)$$
 and $23|(D-10) \Rightarrow 17 \cdot 23|(D-10)$

which gives $D \equiv 10 \pmod{391}$. Thus D = 10.