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

$$\begin{aligned}
11^1 \bmod 645 &= 11 & 123^1 \bmod 101 &= 22\\
11^2 \bmod 645 &= 121 & 123^2 \bmod 101 &= 22^2 \bmod 101 = 80\\
11^4 \bmod 645 &= 121^2 \bmod 645 = 451 & 123^4 \bmod 101 &= 80^2 \bmod 101 = 37\\
11^8 \bmod 645 &= 451^2 \bmod 645 = 226 & 123^8 \bmod 101 &= 37^2 \bmod 101 = 56\\
11^{16} \bmod 645 &= 226^2 \bmod 645 = 121 & 123^{16} \bmod 101 &= 56^2 \bmod 101 = 5\\
11^{32} \bmod 645 &= 451 & 123^{32} \bmod 101 &= 5^2 \bmod 101 = 25\\
11^{64} \bmod 645 &= 226 & 123^{64} \bmod 101 &= 25^2 \bmod 101 = 19\\
11^{128} \bmod 645 &= 121 & 123^{128} \bmod 101 &= 19^2 \bmod 101 = 58\\
11^{256} \bmod 645 &= 451 & 123^{256} \bmod 101 &= 58^2 \bmod 101 = 31\\
11^{512} \bmod 645 &= 226 & 123^{512} \bmod 101 &= 31^2 \bmod 101 = 52
\end{aligned}$$

Thus
$$11^{644} \bmod 645 = \underbrace{226 \cdot 121}\cdot 451 \bmod 645 = 256 \cdot 451 \bmod 645 = 1$$
and
$$\begin{aligned}
123^{1001} \bmod 101 &= \underbrace{52 \cdot 31}\cdot\underbrace{58 \cdot 19}\cdot\underbrace{25 \cdot 56}\cdot 22 \bmod 101\\
&= \underbrace{97 \cdot 92}\cdot\underbrace{87 \cdot 22} \bmod 101\\
&= 36 \cdot 96 \bmod 101 = 22.
\end{aligned}$$

2. Solve the congruence $2x \equiv 7 \bmod 17$.
It holds $17 = 2 \cdot 8 + 1$ and therefore
$$-8 \cdot 2 \equiv 9 \cdot 2 \equiv 1 \bmod 17.$$
Thus 9 is an inverse of 2 modulo 17. We multiply the congruence with 9 and get
$$2x \equiv 7 \bmod 17 \quad \Leftrightarrow \quad 9 \cdot 2x \equiv 9 \cdot 7 \equiv 12 \bmod 17 \quad \Leftrightarrow \quad x \equiv 9 \cdot 7 \equiv 12 \bmod 17.$$

University of Limerick
Department of Mathematics and Statistics
Dr. S. Franz
OLLSCOIL LUIMNIGH
UNIVERSITY OF LIMERICK

3. Find all solutions to the system of congruences.
$$x \equiv 2 \pmod 3, \quad x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 5.$$
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
$$\begin{aligned}
M_1 &= 60/3 = 20, & 20y_1 \bmod 3 &= 2y_1 \bmod 3 \overset{!}{=} 1 & &\Rightarrow y_1 = 2\\
M_2 &= 60/4 = 15, & 15y_2 \bmod 4 &= 3y_2 \bmod 4 \overset{!}{=} 1 & &\Rightarrow y_2 = 3\\
M_3 &= 60/5 = 12, & 12y_3 \bmod 5 &= 2y_3 \bmod 5 \overset{!}{=} 1 & &\Rightarrow y_3 = 3.
\end{aligned}$$
We get $x \equiv 2 \cdot 2 \cdot 20 + 1 \cdot 3 \cdot 15 + 3 \cdot 3 \cdot 12 \equiv 80 + 45 + 108 \equiv 20 + 45 + 48 \equiv 5 + 48 \equiv 53 \pmod{60}$.

4. Find all solutions, if any, to the system of congruences.
$$x \equiv 5 \pmod 6, \quad x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}.$$
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
$$\begin{aligned}
x \equiv 5 \pmod 6 \quad &\Leftrightarrow x \equiv 1 \pmod 2\\
& x \equiv 2 \pmod 3\\
x \equiv 3 \pmod{10} \quad &\Leftrightarrow x \equiv 1 \pmod 2\\
& x \equiv 3 \pmod 5\\
x \equiv 8 \pmod{15} \quad &\Leftrightarrow x \equiv 2 \pmod 3\\
& x \equiv 3 \pmod 5
\end{aligned}$$
This new system has 6 congruences with redundancies—here the compact version
$$x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5.$$
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
$$k_1 = 5k + 3, \quad k_2 = 3k + 2, \quad k_3 = 2k + 1 \text{ with any integer } k$$
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

$$3^4 \bmod 5 = 1, \quad 3^6 \bmod 7 = 1, \quad 3^{10} \bmod 11 = 1.$$

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

$$\begin{aligned} 3^{302} &\equiv 3^2 \cdot (3^4)^{75} \equiv 9 \equiv 4 \pmod 5, \\ 3^{302} &\equiv 3^2 \cdot (3^6)^{50} \equiv 9 \equiv 2 \pmod 7, \\ 3^{302} &\equiv 3^2 \cdot (3^{10})^{30} \equiv 9 \pmod{11}. \end{aligned}$$

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

$$x \equiv 4{\cdot}3{\cdot}77+2{\cdot}6{\cdot}55+9{\cdot}6{\cdot}35 \equiv 924+660+1890 \equiv 154+275+350 \equiv 779 \equiv 9 \pmod{385}.$$

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.

$$\begin{aligned} 352 &= 31 \cdot 11 + 11 & 11 &= 351 - 31 \cdot 11 \\ 31 &= 11 \cdot 2 + 9 & 9 &= 31 - 11 \cdot 2 \\ 11 &= 9 \cdot 1 + 2 & 2 &= 11 - 9 \cdot 2 \\ 9 &= 2 \cdot 4 + 1 & 1 &= 9 - 2 \cdot 4 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

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

$$\begin{aligned} 101^1 \bmod 391 &= 101 \\ 101^2 \bmod 391 &= 35 \\ 101^4 \bmod 391 &= 35^2 \bmod 391 = 52 \\ 101^8 \bmod 391 &= 52^2 \bmod 391 = 358 \\ 101^{16} \bmod 391 &= 358^2 \bmod 391 = 307 \end{aligned}$$

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

$$\begin{aligned} 250^{159} \bmod 17 &= 12^{159} \bmod 17 = 12^{15}(12^{16})^9 \bmod 17 = 12^{15} \bmod 17 = 10 \\ 250^{159} \bmod 23 &= 20^{159} \bmod 23 = 20^5(20^{22})^7 \bmod 23 = 20^5 \bmod 23 = 10 \end{aligned}$$

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

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

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

$$17 | (D - 10) \text{ and } 23 | (D - 10) \quad \Rightarrow \quad 17 \cdot 23 | (D - 10)$$

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