

## Computer Tutorial 12

1. MAGMA can solve Chinese Remainder Theorem problems: if  $n$  and  $m$  are coprime positive integers then `CRT([a,b],[n,m])` will return a number that is congruent to  $a \pmod n$  and congruent to  $b \pmod m$ . Use this function to solve the simultaneous congruences  $x \equiv 573 \pmod{1001}$  and  $x \equiv 2 \pmod{999}$ . Use `mod` to check the answer.
2. Put  $m = 425257806103696493$ . Use MAGMA's `factorization` function to find the prime factors of  $m$ . Then solve  $x^2 \equiv 361971017277558996 \pmod m$ . (Do this by first finding the number  $r$  that is the residue of  $361971017277558996 \pmod p$  and the number  $s$  that is the residue of  $361971017277558996 \pmod q$ , where  $p$  and  $q$  are the prime factors of  $m$ , then solving  $x^2 \equiv r \pmod p$  and  $x^2 \equiv s \pmod q$ , and then using the CRT function to get all four square roots.)
3. Using the same  $m$  as in the previous exercise, solve  $x^2 \equiv 139642041051408538 \pmod m$ . (This time when you come to solve  $x^2 \equiv r \pmod p$  and  $x^2 \equiv s \pmod q$  make use of the fact that  $p$  and  $q$  are both congruent to  $3 \pmod 4$ . (So, for example,  $r^{\frac{1}{4}(p+1)}$  is a square root of  $r \pmod p$ . Use `r:= 139642041051408538 mod p;` followed by `Modexp(r, (p+1) div 4, p);`, etc.. Or, in fact, `Modexp(139642041051408538, (p+1) div 4, p);` would do just as well.)
4. Type `load "tut12data.txt";`. This defines two primes  $p_1$  and  $p_2$ . Type `p1;` and `p2;` to see them, and then check that they are both congruent to  $3 \pmod 4$ .

Suppose that you are a user of Rabin's public key cryptosystem and  $\langle p_1, p_2 \rangle$  is your private key. Thus your public key is  $mm := p_1 * p_2$ . Suppose further that you have received a message (allegedly sent to you by Oscar Wilde). This message consists of a sequence of residues mod  $mm$ , and since it has been included in the file `tut12data.txt` that you have just loaded, you can see the ciphertext by typing `message;`. You will see that in fact `message` has exactly two terms (which you can obtain separately as `message[1];` and `message[2];`).

Find a square root of `message[1] (mod mm)`, via the commands

```
m11:=Modexp(message[1], (p1+1) div 4, p1);  
m12:=Modexp(message[1], (p2+1) div 4, p2);  
m1:=CRT([m11,m12],[p1,p2]);
```

and see if it is the right square root by trying `NaiveDecoding([m1]);`. If you get a MAGMA error, try another square root (by modifying the CRT command). Then do the same for `message[2]`. When you have the right square roots  $m_1$  and  $m_2$  you can get the whole message in its original form via `NaiveDecoding([m1,m2]);`.

5. Let  $p = 65537 = 2^{16} + 1$ . It happens that  $p$  is a prime.

Note that  $(p-1)/2 = 2^{15} = 32768$ . Type `Modexp(500,32768,65537);`. Why does the answer enable you to deduce that 500 is a primitive root mod  $p$ ?

Since 500 is a primitive root, there must a positive integer  $i$  less than 65536 such that  $500^i \equiv 23 \pmod{p}$ . The integer  $i$  can be found by using the Pohlig-Hellman algorithm. Your task is to do this (using MAGMA as a calculator).

You will need pen and paper as well as MAGMA.

Use `Modexp(23,32768,65537);` to check that  $23^{32768} \equiv 65536 \pmod{65537}$ . So if  $23 \equiv 500^i \pmod{65537}$  then  $(500^{32768})^i \equiv 65536 \pmod{65537}$ . You can deduce from this that  $i$  is odd. (Why?)

Given now that  $i = 2j + 1$  for some  $j$ , the congruence  $500^i \equiv 23$  gives  $500^{2j} \equiv 23 \times 500^{-1} \pmod{p}$ . Compute the right hand side via `23*Modexp(500,-1,65537) mod 65537;`. You will find that the answer is 15860. The next thing to do is `Modexp(15860,16384,65537);`. The answer is 65536, and so  $(500^{2j})^{16384} \equiv 65536 \pmod{p}$ . Why does this tell you that  $j$  is odd, and (hence) that  $i = 4k + 3$  for some  $k$ ?

From  $i = 4k + 3$  it follows that  $500^{4k} \equiv 23 \times 500^{-3} \pmod{p}$ . So the next thing to do is `23*Modexp(500,-3,65537) mod 65537;`. The answer is 57206, and the next command you need is `Modexp(57206,8192,65537);` (finding the residue of  $(500^{4k})^{8192} \pmod{p}$ ). The answer tells you that  $k = 2m$  for some  $m$ . Why? And why should you now continue with the command `Modexp(57206,4096,65537);`? The answer tells you that  $m$  is even, and hence that  $i = 16n + 3$  for some  $n$ .

Continue on with calculations like this until you finally prove that  $i$  is congruent to 25283 mod 65536.

You will need to do 11 more steps:

$57206^{2048} \equiv 1$ . So  $n = 2l$ , and  $i = 32l + 3$ .

$57206^{1024} \equiv 1$ . So  $l = 2q$ , and  $i = 64q + 3$ .

$57206^{512} \equiv -1$ . So  $q = 2r + 1$ , and  $i = 128r + 67$ .

We find that  $23 \times 500^{-67} \equiv 49954$ , and  $49954^{256} \equiv -1$ . So  $r = 2s + 1$ , and  $i = 256s + 195$ .

We find that  $23 \times 500^{-195} \equiv 9589$ , and  $9589^{128} \equiv 1$ . So  $s = 2t$ , and  $i = 512t + 195$ .

$9589^{64} \equiv -1$ . So  $t = 2u + 1$ , and  $i = 1024u + 707$ .

We find that  $23 \times 500^{-707} \equiv 16$ , and  $16^{32} \equiv 1$ . So  $u = 2v$ , and  $i = 2048v + 707$ .

$16^{16} \equiv 1$ . So  $v = 2w$ , and  $i = 4096w + 707$ .

$16^8 \equiv 1$ . So  $w = 2x$ , and  $i = 8192x + 707$ .

$16^4 \equiv -1$ . So  $x = 2y + 1$ , and  $i = 16384y + 8899$ .

We find that  $23 \times 500^{-8899} \equiv 65281$ , and  $65281^2 \equiv -1$ . So  $y = 2z + 1$ , and  $i = 32768z + 25283$ .

We now find that  $23 \times 500^{-25283} \equiv 1$ . So  $i = 25283$  solves  $23 \equiv 500^i$ . We are finished!