Mathematics 124 Fall 2003

HOMEWORK ASSIGNMENT # 3
DUE, Friday, October 17

Collaboration: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate, CA, or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class.
Show all your working, and write up your solutions as neatly as possible.

This week's assignment involves some large numbers which can only be handled using computers. One program that does arithmetic with large integers is the programme `pari`. Attached is a brief tutorial with all that you need to know about using `pari`. Moreover, you may not want to copy large numbers directly from the page onto the screen. You can get the numbers digitally by downloading a text version of this assignment on the webpage `http://www.math.harvard.edu/~fcale`.

In the following RSA encryption problem, we code messages into numbers as follows. Using the following table:

Symbol	Code	Symbol	Code	Symbol	Code	Symbol	Code
A	00	K	10	U	20	4	30
B	01	L	11	V	21	5	31
C	02	M	12	W	22	6	32
D	03	N	13	X	23	7	33
E	04	O	14	Y	24	8	34
F	05	P	15	Z	25	9	35
G	06	Q	16	0	26	space	36
H	07	R	17	1	27	.	37
I	08	S	18	2	28		
J	09	T	19	3	29		

Given a message M, translate M into a number by taking the code for each symbol and concatenating. Thus for "12 EGGS", the individual symbols translate into $\{27, 28, 36, 04, 06, 06, 18\}$, which then concatenates to

$$27283604060618.$$

Conversely, 617141818 becomes (taking care to work from right to left) into $\{06, 17, 14, 18, 18\}$ or "GROSS".

1. Gauss Corp. uses an RSA algorithm with the following public key:

$$f : x \to x^5 \mod m$$

with $d = 5$, and $m = 5913594235257971$. Since $m < 10^{16}$, this code can be used for messages of (symbol) length at most 7.

   (a) (1 point) How would the message "RED SOX" be encoded?

   (b) (2 points) Gauss Corp. sends you the following electronic signature: 1200660659783330. Verify this signature.

   (c) (4 points) Break Gauss Corp.'s RSA code. In other words, find the e such that $x^{de} \equiv 1 \mod m$.

2. Euler Corp. uses an RSA algorithm with the following public key:

$$f : x \to x^{13} \mod m'$$

with

$$\begin{aligned} m' = \ & 11679847981112819759721399310592745791658017001955007325132\,9 \\ & 1383783133049588151975645370374287852614884146888067442512\,21 \\ & 9413748768010657572575384986457405973985247465176041951676\,95 \\ & 4461208131403777 \end{aligned}$$

   (a) (8 points) You suspect that Gauss Corp. is trying to break Euler Corp.'s RSA code. You manage to intercept the following two internal coded messages from Gauss Corp:

$$5047420201508299, 5052809437522820$$

   Decode these messages, and follow the clues to find the factorization of m'.

   (b) (5 points) Using the factorization of m', crack Euler Corp.'s RSA algorithm, and use it to decode the following message from Euler Corp.:

$$\begin{aligned} M = \ & 246964778833892955506076498477784766350072590773343913919239 \\ & 588733273351776454938949611079105164265317231894171892238877 \\ & 760102697253972391190044532425369109272485502284832536628712 \\ & 645429341476006 \mod m' \end{aligned}$$

Pari

Start `pari`. For any integers x and m, compute $x \mod m$ by typing:

```
Mod(x,m)
```

To compute x^d modulo m, first compute x modulo m and then raise to the dth power. You can do this all at once by typing

```
Mod(x,m)^d
```

You could do the same thing by typing `Mod(`x^d`,m)`, but this is much slower for large m and d. To solve the equation $de \equiv 1 \mod n$, if you already know d and n, simply compute d^{-1} modulo n, or

```
Mod(d,n)^(-1)
```

Finally, to factor an integer m type

```
factor(m)
```

Factoring will only work if m is sufficiently small. For example, it will not be able to factor the integer m' occurring in the assignment. Some other operations you might want to do include multiplication of two numbers p and q:

```
p*q
```

Note that if you want to multiply $(p-1)$ and $(q-1)$ you must type

```
(p-1)*(q-1)
```

Example

Here is a worked example. Consider the RSA algorithm defined by $x \mapsto x^3 \mod 10807$. First type

```
factor(10807)
%1 =
[101 1]

[107 1]
```

We find that $m = 10807 = 101 \times 107$. Thus $\varphi(m) = 10600$. Thus we need to find an e such that $de \equiv 1 \mod 10600$. Since $d = 3$, type

```
Mod(3,10600)^(-1)
%2 = Mod(7067, 10600)
```

We see the result is 7067, and thus $e = 7067$. To uncode the message 9876, type

```
Mod(9876,10807)^(7067)
%3 = Mod(4031, 10807)
```

The answer is 4031. We can check this is correct, by typing

```
Mod(4031,10807)^3
%4 = Mod(9876 10807)
```

which gives us back 9876.

You can download `pari` for free at
`http://www.gn-50uma.de/ftp/pari/00index.html`
Tell me if you have any problems obtaining this, or problems using `pari`. The best way to contact me and get a quick response is to email me: `fcale@math.harvard.edu`.