Exercises

Exercise 1 : State Fermat's little theorem.

Compute the gcd of

$$2^{1201201201201201201201201201201201201201201201201201201201201201201201201201201201201201201201201201202012}-1$$

and 143.

Exercise 2 :

Factor 143.

Which is the set $\mathcal{S}$ of integers x such that $x^{103} = 2 \bmod 143$?

Exercise 3 :

Let $p = 331$. Prove that p is a prime integer.

Factor $p - 1$.

We have checked that $2^{165} = 330 \bmod p$, $2^{110} = 299 \bmod p$, $2^{66} = 64 \bmod p$, $2^{30} = 1 \bmod p$, $5^{165} = 1 \bmod p$, $5^{110} = 31 \bmod p$, $5^{66} = 64 \bmod p$, $5^{30} = 180 \bmod p$.

Give a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

Set $b = 329 \bmod p$. We have checked that $b^{165} = 1 \bmod p$, $b^{110} = 299 \bmod p$, $b^{66} = 64 \bmod p$, $b^{30} = 1 \bmod p$.

Using the method of Pohlig-Hellman compute an integer ℓ such that $5^{\ell} \bmod p$.

Exercise 4 :

Let $f(x)$ be the polynomial $x^5 + x^4 + 1$ in $\mathbb{F}_2[x]$.

Factor $f(x)$.

Set $\mathbf{K} = \mathbb{F}_2[x]/f(x)$.

Is $\mathbf{K}$ a field ?

Solve the equation $a^{11} = x \bmod f(x)$ where the unknown a belongs to $\mathbf{K}$.

Exercise 5 :

Let

$$n=2\times 3^{72}\times 5^{94}+1=2274787028249772486776426616646752916803470356294752032920609974286918486541253514587879180908203125 1.$$

How would you compute $2^{(n-1)/2} \bmod p$ with a computer ? How much time would it take ?

We have computed

$$2^{(n-1)/2}=22747870282497724867764266166467529168034703562947520329206099742869184865412535145878791809082031250 \bmod n.$$

And

$$2^{(n-1)/3}=11791219678163940506615639138405431889788864963308512559814102611481363493589902969729020027163691504 \bmod n,$$

$$2^{(n-1)/5}=21654376330887561819730743112521290573534764125875638216950517656429881743275862730524129927387779523 \bmod n.$$

Is n a prime or a composite integer ?

Let

$$m=2\times 3^{72}\times 5^{93}+1=4549574056499544973552853233293505833606940712589504065841219948573836973082507029175758361816406251.$$

We have computed

$$2^{(m-1)/2}=3281530472308397151367076951503834499443980341212687665140461391271486606177374329391467659758034415 \bmod m,$$

$$2^{(m-1)/3}=4382280690852380175557117046134573047179631520157991376672365344267964597541850193105695293600978651 \bmod m,$$

$$2^{(m-1)/5}=4541219320421909602451780644029122837067788032240411930448399026474063435195377076202995533799648080 \bmod m.$$

Is m a prime or a composite integer ?

Exercise 6 :

Give an algorithm to compute square roots modulo a prime congruent to 3 modulo 4.

We want to prove that there are infinitely many prime integers congruent to 3 modulo 4.

Assume there are only finitely many of them and call them p_i for $1 \leqslant i \leqslant I$.

Set $P = 4 \times \prod_{1\leq i\leq I} p_i - 1$

Prove that one at least of the prime divisors of P is congruent to 3 modulo 4. Call it q.

Prove that q is not equal to any of the p_i. Conclude.

Exercise 7 :

Find, if it exists, an integer n that is congruent to 5 modulo 6, to 11 modulo 15, and to 1 modulo 10.

Find, if it exists, an integer n that is congruent to 1 modulo 2, to -1 modulo 3, to 3 modulo 5, to 4 modulo 7.

Exercise 8 :

We want to factor the integer $N = 32399$ using the quadratic sieve.

1 . We notice that $\sqrt{N} \simeq 179.9$. Write a congruence modulo N of the type

$$(a+m)^2 \equiv a^2 + u_1 a + u_0 \bmod N$$

depending on an integer parameter a. Here m, u_0, u_1 are well chosen integer constants.

2 . Find values of a in the interval $[-40, 40]$ that produce a congruence between a square and a smooth number (in a sense to be made precise) modulo N. You may use the following data.

```
for(a=-40,40,print([a,factor(a^2+2*a*180+1)]))
[-40, [-1, 1; 12799, 1]]
[-39, [-1, 1; 2, 1; 11, 1; 569, 1]]
[-38, [-1, 1; 5, 1; 2447, 1]]
[-37, [-1, 1; 2, 1; 5, 2; 239, 1]]
[-36, [-1, 1; 107, 1; 109, 1]]
[-35, [-1, 1; 2, 1; 11, 2; 47, 1]]
[-34, [-1, 1; 11083, 1]]
[-33, [-1, 1; 2, 1; 5, 1; 13, 1; 83, 1]]
[-32, [-1, 1; 5, 1; 2099, 1]]
[-31, [-1, 1; 2, 1; 5099, 1]]
[-30, [-1, 1; 19, 1; 521, 1]]
[-29, [-1, 1; 2, 1; 4799, 1]]
[-28, [-1, 1; 5, 1; 11, 1; 13, 2]]
[-27, [-1, 1; 2, 1; 5, 1; 29, 1; 31, 1]]
[-26, [-1, 1; 19, 1; 457, 1]]
[-25, [-1, 1; 2, 1; 53, 1; 79, 1]]
[-24, [-1, 1; 11, 1; 733, 1]]
[-23, [-1, 1; 2, 1; 5, 3; 31, 1]]
[-22, [-1, 1; 5, 1; 1487, 1]]
[-21, [-1, 1; 2, 1; 3559, 1]]
[-20, [-1, 1; 13, 1; 523, 1]]
[-19, [-1, 1; 2, 1; 41, 1; 79, 1]]
[-18, [-1, 1; 5, 1; 1231, 1]]
[-17, [-1, 1; 2, 1; 5, 1; 11, 1; 53, 1]]
[-16, [-1, 1; 5503, 1]]
[-15, [-1, 1; 2, 1; 13, 1; 199, 1]]
[-14, [-1, 1; 29, 1; 167, 1]]
[-13, [-1, 1; 2, 1; 5, 1; 11, 1; 41, 1]]
[-12, [-1, 1; 5, 2; 167, 1]]
[-11, [-1, 1; 2, 1; 19, 1; 101, 1]]
[-10, [-1, 1; 3499, 1]]
[-9, [-1, 1; 2, 1; 1579, 1]]
[-8, [-1, 1; 5, 1; 563, 1]]
[-7, [-1, 1; 2, 1; 5, 1; 13, 1; 19, 1]]
[-6, [-1, 1; 11, 1; 193, 1]]
[-5, [-1, 1; 2, 1; 887, 1]]
[-4, [-1, 1; 1423, 1]]
[-3, [-1, 1; 2, 1; 5, 1; 107, 1]]
[-2, [-1, 1; 5, 1; 11, 1; 13, 1]]
[-1, [-1, 1; 2, 1; 179, 1]]
[0, matrix(0,2)]
[1, [2, 1; 181, 1]]
[2, [5, 2; 29, 1]]
[3, [2, 1; 5, 1; 109, 1]]
[4, [31, 1; 47, 1]]
[5, [2, 1; 11, 1; 83, 1]]
```

```
[6, Mat([13, 3])]
[7, [2, 1; 5, 1; 257, 1]]
[8, [5, 1; 19, 1; 31, 1]]
[9, [2, 1; 11, 1; 151, 1]]
[10, Mat([3701, 1])]
[11, [2, 1; 13, 1; 157, 1]]
[12, [5, 1; 19, 1; 47, 1]]
[13, [2, 1; 5, 2; 97, 1]]
[14, Mat([5237, 1])]
[15, [2, 1; 29, 1; 97, 1]]
[16, [11, 1; 547, 1]]
[17, [2, 1; 5, 1; 641, 1]]
[18, [5, 1; 1361, 1]]
[19, [2, 1; 13, 1; 277, 1]]
[20, [11, 1; 691, 1]]
[21, [2, 1; 4001, 1]]
[22, [5, 1; 41, 2]]
[23, [2, 1; 5, 1; 881, 1]]
[24, [13, 1; 709, 1]]
[25, [2, 1; 4813, 1]]
[26, Mat([10037, 1])]
[27, [2, 1; 5, 2; 11, 1; 19, 1]]
[28, [5, 1; 41, 1; 53, 1]]
[29, [2, 1; 5641, 1]]
[30, Mat([11701, 1])]
[31, [2, 1; 11, 1; 19, 1; 29, 1]]
[32, [5, 1; 13, 1; 193, 1]]
[33, [2, 1; 5, 1; 1297, 1]]
[34, Mat([13397, 1])]
[35, [2, 1; 31, 1; 223, 1]]
[36, [53, 1; 269, 1]]
[37, [2, 1; 5, 1; 13, 1; 113, 1]]
[38, [5, 3; 11, 2]]
[39, [2, 1; 31, 1; 251, 1]]
[40, Mat([16001, 1])]
```

3 . Write down all the congruences you have found. Report the signs and valuations in a matrix M with integer coefficients.

4 . Compute (a basis of) the kernel of the reduction modulo 2 of the matrix M.

5 . For each vector in this basis write a congruence between two squares modulo N. Deduce a factorization of N.

Exercise 9 :

Recall the definition of the Legendre symbol. Recall the definition of the Jacobi symbol. State the quadratic reciprocity law. Compute the Jacobi symbol $\left(\frac{4673}{5352499}\right)$.
