CoCoNuT Assignment Two

January 15, 2015

1 More Sage

Groups of integers modulo n are created with the `Integers` command. You can then use the group name to map an integer into the group. You can use the usual addition and multiplication operations and `-a` and `1/a` for inversion in the additive resp. multiplicative groups.

```
sage: G=Integers(7)
sage: a=G(5)
sage: b=G(2)
sage: a+b
0
sage: -a
2
sage: 1/a
3
```

Vectors and matrices work as one would expect. To use matrices over a structure (such as a group), use the

`MatrixSpace(struct,rows,cols)`

constructor. The `^-1` operation inverts a matrix, if possible.

```
sage: v=vector([1,2,3])
sage: w=vector([1,1,0])
sage: v+w
(2, 3, 3)

sage: m=matrix([[1,2],[3,4]])
sage: n=identity_matrix(2)
sage: m+n
[2 2]
[3 5]
sage: m*n
[1 2]
[3 4]

sage: M=MatrixSpace(Integers(5),2,2)
sage: M([[2,3],[3,2]])+M([[4,2],[1,2]])
[1 0]
[4 4]

sage: M([[2,1],[1,2]])^-1
```

```
[4 3]
[3 4]
```

Elliptic curve groups are useful in number theory and cryptography. The basic idea is to start with the set of points (x, y) satisfying an equation of the form[1] $y^2 = x^3 + ax + b$ where all computation is done modulo a prime p. We then add a "point at infinity" $\mathcal{Z}$ as a neutral element, i.e. $\mathcal{Z} + \mathcal{Z} = \mathcal{Z}$ and $\mathcal{Z} + (x, y) = (x, y) = (x, y) + \mathcal{Z}$ for all points (x, y) on the curve. It turns out that this gives a group for a particular addition law. All we need to know for now is that these points form a group and the sage command to generate such a group is `EllipticCurve(P, [a, b])` where `P` is the structure of integers modulo p.

```
sage: E=EllipticCurve(Integers(7),[3, 1])
sage: E
Elliptic Curve defined by y^2 = x^3 + 3*x + 1 over
         Ring of integers modulo 7
```

Sage outputs elliptic curve points in the format `(x:y:1)` or `(0:1:0)` for the point at infinity (there are reasons for this format, which do not concern us here). To input the point at infinity we use `E(0)`.

```
sage: E([5, 1])
(5 : 1 : 1)
sage: E(0)
(0 : 1 : 0)
sage: E([5,1])+E([5,1])
(6 : 2 : 1)
sage: E([5,1])+E(0)
(5 : 1 : 1)
sage: -E([5,1])
(5 : 6 : 1)
sage: E([5,1])+E([5,6])
(0 : 1 : 0)
```

[1]For this to work, the discriminant $\Delta = 4a^3 + 27b^2$ must be nonzero. Also for simplicity, we assume $p > 3$ as the cases $p = 2, 3$ have some exceptions to the rules given here.

2 Assignment Two Questions

1. Consider the following groups:

   (a) The group of 3×2 matrices modulo 4 with matrix addition as the group operation.

   (b) The group of invertible 2×2 matrices modulo 3 with matrix multiplication as the group operation.

   (c) The group of permutations of the set $S = \{0, 1, 2, 3, 4\}$.

   For each group, find

   (a) The neutral element.

   (b) The group order.

   (c) Is the group Abelian?

   (d) A generator, if one exists.

2. (a) Find the order of the group of the elliptic curve given by $a = 7$ and $b = 3$ modulo $p = 1009$.

   (b) Is the above group Abelian?

   (c) Write a function that takes an elliptic curve point P and an integer n and adds P to itself n times, using only the group structure of the curve and commands from the previous assignment.

   (d) Use your algorithm to compute $512 \cdot (9064, 6692)$ on the curve defined by $a = 11, b = 4$ modulo $p = 10037$.

3. Give an algorithm that takes a permutation as a $2 \times n$ matrix (as in the lecture notes) and outputs it as a list of disjoint cycles. Do not use sage's permutation group library.

4. (a) Write a function that takes as input integers a, b, c and finds a solution to the equation $a^x = b \pmod{c}$. (You will have to do an exhaustive search given what you currently know.)

(b) Solve $34091202317940^x = 46461034929471 \bmod 61704897745301$.

(c) Adapt your algorithm from part a) above as necessary for the case of an elliptic curve group.

(d) Solve the equation $x \cdot P = Q$ on the elliptic curve defined by $a = 5, b = 1$ modulo $p = 138451$ with $P = (74030, 23679)$ and $Q = (33643, 90060)$.