

## Homework Set 11

### Problem 1

**Example 28.** Among 20 people (no leaplings), what is the probability that two have the same birthday?

**Solution.** The probability is

$$1 - \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\left(1 - \frac{3}{365}\right)\cdots\left(1 - \frac{19}{365}\right) \approx 0.411438.$$

[Or, equivalently, about 41.14%.]

### Problem 2

**Example 29.** Consider the elliptic curve  $y^2 = x^3 + 3x + 5$  as well as the points  $P = (4, 9)$  and  $Q = (1, 3)$  on that curve. Determine  $P \boxplus Q$ .

**Solution.** We let Sage do the work for us:

```
>>> E = EllipticCurve([3,5])
```

```
>>> E(4,9) + E(1,3)
```

```
(-1:1:1)
```

We conclude that  $P \boxplus Q = (-1, 1)$ .

### Problem 3

**Example 30.** Consider the elliptic curve  $y^2 = x^3 + 7x + 4$  as well as the point  $P = (0, 2)$  on that curve.

(a) Determine  $2P$ .

(b) Determine  $3P$ .

**Solution.** We let Sage do the work for us:

```
>>> E = EllipticCurve([7,4])
```

```
>>> 2*E(0,2)
```

```
( $\frac{49}{16}, -\frac{471}{64}, 1$ )
```

```
>>> 3*E(0,2)
```

```
( $\frac{15072}{2401}, \frac{2021734}{117649}, 1$ )
```

We conclude that  $2P = \left(\frac{49}{16}, -\frac{471}{64}\right)$  and  $3P = \left(\frac{15072}{2401}, \frac{2021734}{117649}\right)$ .

## Problem 4

**Example 31.** Consider the elliptic curve  $y^2 = x^3 + 3x + 2$  modulo 5. List all points  $(x, y)$ .

**Solution.** Note that, because we are working modulo 5, there are only 5 possible values for  $x$ . Hence, we can go through all possibilities for  $x$  and determine the corresponding possible values for  $y$ :

- $x = 0$ :  $y^2 = 0^3 + 3 \cdot 0 + 2 = 2$  has no solutions.
- $x = 1$ :  $y^2 = 1^3 + 3 \cdot 1 + 2 \equiv 1$  has solutions  $y \equiv \pm 1$ , resulting in the points  $(1, \pm 1)$ .
- $x = 2$ :  $y^2 = 2^3 + 3 \cdot 2 + 2 \equiv 1$  has solutions  $y \equiv \pm 1$ , resulting in the points  $(2, \pm 1)$ .
- $x = -2$ :  $y^2 = (-2)^3 + 3 \cdot (-2) + 2 \equiv -2$  has no solutions.
- $x = -1$ :  $y^2 = (-1)^3 + 3 \cdot (-1) + 2 \equiv -2$  has no solutions.

Overall, we have found the points  $(1, \pm 1)$ ,  $(2, \pm 1)$ , for a total of 5 points if we include the special point  $O$ .

**Sage.** Alternatively, we can let Sage do this work for us:

```
>>> E = EllipticCurve(GF(5), [3,2])
>>> E.points()
[(0:1:0), (1:1:1), (1:4:1), (2:1:1), (2:4:1)]
```

## Problem 5

**Example 32.** Consider the elliptic curve  $y^2 = x^3 + 9x + 5$  modulo 43 as well as the point  $P = (3, 4)$  on that curve.

- Determine  $2P$ .
- Determine  $3P$ .

**Solution.** We let Sage do the work for us:

```
>>> E = EllipticCurve(GF(43), [9,5])
>>> 2*E(3,4)
(25:26:1)
>>> 3*E(3,4)
(16:26:1)
```

We conclude that  $2P = (25, 26)$  and  $3P = (16, 26)$ .