We get the same numbers. This is simply the fact mentioned previously that the addition of points on the curve corresponds to multiplication of the corresponding numbers. Moreover, note that \(45 \equiv 1 \pmod{11}\), but not \(13\). This corresponds to the fact that 5 times the point \((-1, 2)\) is \(\infty \pmod{11}\) but not \(\infty \pmod{13}\). Note that 1 is the multiplicative identity for multiplication \(\pmod{11}\), while \(\infty\) is the additive identity for addition on the curve.

It is easy to see from the preceding that factorization using the curve \(y^2 = x^3 - 3x + 2\) is essentially the same as using the classical \(p-1\) factorization method (see Section 6.4).

In the preceding example, the cubic equation had a double root. An even worse possibility is the cubic having a triple root. Consider the curve

\[ y^2 = x^3. \]

To a point \((x, y) \neq (0, 0)\) on this curve, associate the number \(x/y\). Let's start with the point \(P = (1, 1)\) and compute its multiples:

\[ P = (1, 1), \quad 2P = \left(\frac{1}{4}, \frac{1}{8}\right), \quad 3P = \left(\frac{1}{9}, \frac{1}{27}\right), \ldots, \quad mP = \left(\frac{1}{m^2}, \frac{1}{m^3}\right). \]

Note that the corresponding numbers \(x/y\) are 1, 2, 3, \ldots, \(m\). Adding the points on the curve corresponds to adding the numbers \(x/y\).

If we are using the curve \(y^2 = x^3\) to factor \(n\), we need to change the points \(mP\) to integers \(\pmod{n}\), which requires finding inverses for \(m^2\) and \(m^3 \pmod{n}\). This is done by the extended Euclidean algorithm, which is essentially a \(\gcd\) computation. We find a factor of \(n\) when \(\gcd(m, n) \neq 1\). Therefore, this method is essentially the same as computing in succession \(\gcd(2, n), \gcd(3, n), \gcd(4, n), \ldots\) until a factor is found. This is a slow version of trial division, the oldest factorization technique known. Of course, in the elliptic curve factorization algorithm, a large multiple \((B!)P\) of \(P\) is usually computed. This is equivalent to factoring by computing \(\gcd(B!, n)\), a method that is often used to test for prime factors up to \(B\).

In summary, we see that the \(p-1\) method and trial division are included in the elliptic curve factorization algorithm if we allow degenerate curves.

### 15.4 Elliptic Curves in Characteristic 2

Many applications use elliptic curves \(\pmod{2}\), or elliptic curves defined over the finite fields \(GF(2^n)\) (these are described in Section 3.10). This is often because \(\pmod{2}\) adapts well to computers.

If we're working \(\pmod{2}\), the equations for elliptic curves need to be modified slightly. There are many reasons for this. For example, the derivative
of $y^2$ is $2yy' = 0$, since 2 is the same as 0. This means that the tangent lines we compute are vertical, so $2P = \infty$ for all points $P$. A more sophisticated explanation is that the curve $y^2 \equiv x^3 + ax + b \pmod{2}$ has singularities (points where the partial derivatives with respect to $x$ and $y$ simultaneously vanish).

The equations we need are of the form

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_1, \ldots, a_6$ are constants. The addition law is slightly more complicated. We still have three points adding to infinity if and only if they lie on a line. Also, the lines through $\infty$ are vertical. But, as we'll see in the following example, finding $-P$ from $P$ is not as the same as before.

**Example.** Let $E : y^2 + y \equiv x^3 + x \pmod{2}$. As before, we can list the points on $E$

$$(0,0), \quad (0,1), \quad (1,0), \quad (1,1), \quad \infty.$$

Let's compute $(0,0) + (1,1)$. The line through these two points is $y = x$. Substituting into the equation for $E$ yields $x^2 + x \equiv x^3 + x$, which can be rewritten as $x^2(x + 1) \equiv 0$. The roots are $x = 0, 0, 1 \pmod{2}$. Therefore, the third point of intersection also has $x = 0$. Since it lies on the line $y = x$, it must be $(0,0)$. (This might be puzzling. What is happening is that the line is tangent to $E$ at $(0,0)$ and also intersects $E$ in the point $(1,1)$.) As before, we now have

$$(0,0) + (0,0) + (1,1) = \infty.$$

To get $(0,0) + (1,1)$ we need to compute $\infty - (0,0)$. This means we need to find $P$ such that $P + (0,0) = \infty$. A line through $\infty$ is still a vertical line. In this case, we need one through $(0,0)$, so we take $x = 0$. This intersects $E$ in the point $P = (0,1)$. We conclude that $(0,0) + (0,1) = \infty$. Putting everything together, we see that

$$(0,0) + (1,1) = (0,1).$$

In most applications, elliptic curves mod 2 are not large enough. Therefore, elliptic curves over finite fields are used. For an introduction to finite fields, see Section 3.10. However, in the present section, we only need the field $GF(4)$, which we now describe.

Let

$$GF(4) = \{0, 1, \omega, \omega^2\},$$

with the following laws
1. \(0 + x = x\) for all \(x\)
2. \(x + x = 0\) for all \(x\)
3. \(1 \cdot x = x\) for all \(x\)
4. \(1 + \omega = \omega^2\).
5. Addition and multiplication are commutative and associative, and the distributive law holds: \(x(y + z) = xy + xz\) for all \(x, y, z\).

Since \(\omega^3 = \omega \cdot \omega^2 = \omega \cdot (1 + \omega) = \omega + \omega^2 = \omega + (1 + \omega) = 1\), we see that \(\omega^2\) is the multiplicative inverse of \(\omega\). Therefore, every nonzero element of \(GF(4)\) has a multiplicative inverse.

Elliptic curves with coefficients in finite fields are treated just like elliptic curves with integer coefficients.

**Example.** Consider \(E : y^2 + xy = x^3 + \omega\), where \(\omega \in GF(4)\) as before. Let’s list the points of \(E\) with coordinates in \(GF(4)\):

- \(x = 0 \Rightarrow y^2 = \omega \Rightarrow y = \omega^2\)
- \(x = 1 \Rightarrow y^2 + y = 1 + \omega = \omega^2 \Rightarrow \text{no solutions}\)
- \(x = \omega \Rightarrow y^2 + \omega y = 0 \Rightarrow y = 1, \omega^2\)
- \(x = \omega^2 \Rightarrow y^2 + \omega^2 y = 1 + \omega = \omega^2 \Rightarrow \text{no solutions}\)
- \(x = \infty \Rightarrow y = \infty\)

The points on \(E\) are therefore

\[
(0, \omega^2), \quad (\omega, 1), \quad (\omega, \omega^2), \quad \infty
\]

Let’s compute \((0, \omega^2) + (\omega, \omega^2)\). The line through these two points is \(y = \omega^2\). Substitute this into the equation for \(E\):

\[
\omega^4 + \omega^2 x = x^3 + \omega,
\]

which becomes \(x^3 + \omega^2 x = 0\). This has the roots \(x = 0, \omega, \omega^2\). The third point of intersection of the line and \(E\) is therefore \((\omega, \omega^2)\), so

\[
(0, \omega^2) + (\omega, \omega^2) + (\omega, \omega^2) = \infty
\]
15.5 Elliptic Curve Cryptosystems

We need $-(\omega, \omega^2)$, namely the point $P$ with $P + (\omega, \omega^2) = \infty$. The vertical line $x = \omega$ intersects $E$ in $P = (\omega, 1)$, so

$$(0, \omega^2) + (\omega, \omega^2) = (\omega, 1)$$

For cryptographic purposes, elliptic curves are used over fields $GF(2^n)$ with $n$ large, say at least 150.

15.5 Elliptic Curve Cryptosystems

Elliptic curves versions exist for many cryptosystems, in particular those involving discrete logarithms. An advantage of elliptic curves over working with integers mod $p$ is the following. In the integers, it is possible to use the factorization into primes (especially small primes) to attack the discrete logarithm problem. This is known as the index calculus and is described in Section 7.2. There seems to be no good analog of this method for elliptic curves. Therefore, it is possible to use smaller primes, or smaller finite fields, with elliptic curves and achieve a level of security comparable to that for much larger integers mod $p$. This allows great savings in hardware implementations, for example.

In the following, we describe three elliptic curve versions of classical algorithms. As we will see, there is a general procedure for changing a classical system based on discrete logarithms into one using elliptic curves:

1. Change modular multiplication to addition of points on an elliptic curve.

2. Change modular exponentiation to multiplying a point on an elliptic curve by an integer.

Of course, the second situation above is really a special case of the first, since exponentiation consists of multiplying a number by itself several times, and multiplying a point by an integer is adding the point to itself several times.

An Elliptic Curve ElGamal Cryptosystem

We recall the non-elliptic curve version. Alice wants to send a message $x$ to Bob, so Bob chooses a large prime $p$ and an integer $\alpha \mod p$. He also chooses a secret integer $a$ and computes $\beta \equiv \alpha^a \pmod{p}$. Bob makes $p$, $\alpha$, $\beta$ public and keeps $a$ secret. Alice chooses a random $k$ and computes $y_1$ and $y_2$, where

$$y_1 \equiv \alpha^k \quad \text{and} \quad y_2 \equiv x\beta^k \pmod{p}$$