Math 116 HW 7 Jun Ryu

1) $19 = \underbrace{2^4}_{16} + \underbrace{2^2}_{4} - \underbrace{2^0}_{1}$

$\Rightarrow$ 3 terms ✓

2) a) Bob computes the point

$$Q_B = n_B P = 1943 \cdot (1980, 431)$$

$$= \boxed{(1432, 667)} \in E(\mathbb{F}_{2671})$$

```
In [12]: E = EllipticCurve(GF(2671),[171,853])
         P = E.point([1980,431])
         1943*P

Out[12]: (1432 : 667 : 1)
```

b) Calculate the shared secret point:

$$n_B Q_A = 1943 \cdot (2110, 543)$$

$$= (2424, 911) \in E(\mathbb{F}_{2671})$$

```
In [13]: Q = E.point([2110,543])
         1943*Q

Out[13]: (2424 : 911 : 1)
```

Now, they discard the y-coordinate to get that their secret shared value is **2424**

c) We have that $n_A \cdot P = Q_A$, so

```
In [16]: E = EllipticCurve(GF(2671),[171,853])
         P = E.point([1980,431])
         QA = E.point([2110,543])
         QA_guess = P
         nA_guess = 1
         while QA_guess != QA:
             QA_guess = QA_guess + P
             nA_guess += 1

         nA_guess

Out[16]: 726
```

This gives us that $n_A = \boxed{726}$

d) Bob will compute $Q_B = 875 \cdot (1980, 431)$
$= (161, 2040) \in E(\mathbb{F}_{2671})$.

Bob will also only send the x-coordinate $\boxed{x_B = 161}$ to Alice.

Now, we calculate the shared value:

$y_A^2 = x_A^3 + 171 x_A + 853$ and use $x_A = 2$

$2^3 + 171(2) + 853 = 1203.$

So, $y_A = 1203^{(2671+1)/4} = 1203^{668} \equiv 2575 \pmod{2671}$

So, the shared point is

$n_B(x_A, y_A) = 875(2, 2575)$

$= (1708, 1419) \in E(\mathbb{F}_{2671})$

Thus, the secret shared value is $\boxed{1708}$

```
In [14]: 875*P

Out[14]: (161 : 2040 : 1)

In [15]: R = E.point([2,2575])
         875*R

Out[15]: (1708 : 1419 : 1)
```

3)

```
In [1]: F = Zmod(589)
        E = EllipticCurve(F,[4,9])
        P = E.point([2,5])

        print(P, factorial(2)*P,factorial(3)*P,factorial(4)*P)

        (2 : 5 : 1) (564 : 156 : 1) (33 : 460 : 1) (489 : 327 : 1)
```

We have that this throws an error when we try to compute $5! \cdot P$, so we look into that case.

$5! \cdot P = 5 \cdot 4! \cdot P = 5 \cdot (489, 327)$

$= 4 \cdot (489, 327) + (489, 327) \pmod{589}$

$= (223, 61) + (489, 327)$

So, we need the reciprocal of $223 - 489 \pmod{589}$, but

```
In [4]: gcd(223-489,589)
Out[4]: 19
```

, so 19 is a factor,

and we see that $589 = \boxed{19 \cdot 31}$ ✓