Jeremy Barthélemy
ECE 746
Hw. 4

1.
a. A requirement is that we have $y^2 = x^3 + ax + b$ such that $4a^3 + 27b^2$ is not congruent with 0 mod P.
To prove that we satisfy this condition consider our equation:
$y^2 = x^3 + x + 6 \bmod 11$
For this case, a = 1, and b = 6. Thus $4*1 + 27*6^2$ mod 11= (4 + 27*36) mod 11 = 8, which is not equal to zero, and thus our condition is satisfied.
b. We perform the following calculations below:
(2, 7) + (5, 2), and
the doubling of (3, 6).
In order to calculate (2, 7) + (5, 2), the following calculation is first used for λ:
$(y_Q-y_P)*(x_Q-x_P)^{-1}$ mod P
Taking P = (2, 7) and Q = (5, 2), we have λ = $(2-7)*(5-2)^{-1}$ mod 11 = $-5*3^{-1}$ mod 11 =
6 * 4 mod 11 = 2
$x_R = \lambda^2 – x_P – x_Q$ mod 11 = 2^2 - 2 - 5 mod 11 = 4 – 7 mod 11 = -3 mod 11 = 8
$y_R = \lambda(x_P-x_R) – y_P$ mod 11 = 2(2 – 8) – 7 mod 11 = -12 - 7 mod 11 = 3
For our first calculation, (2, 7) + (5, 2) = (8, 3)
Next, we need to double (3, 6):
We use the following equation to calculate lamda:
$(3x_P^2 + a) * (2y^P)^{-1}$ mod 11 = $(3*3*3 + 1) * (2*6)^{-1}$ mod 11 = $28*12^{-1}$ mod 11 = 6*1 mod 11 = 6
$x_R = \lambda^2 – x_P – x_Q$ mod 11 = 6^2 – 3 – 3 mod 11 = 36 -6 mod 11 = 8
$y_R = \lambda(x_P-x_R) – y_P$ mod 11 = 6(3-8) – 6 mod 11 = 6*-5 – 6 mod 11 = -30 – 6 mod 11 = 8
Thus, we fine that by doubling (3, 6), our result is (8, 8).

2.
```
E = EllipticCurve(GF(11),[0, 0, 0, 1, 6])
E.short_weierstrass_model()

#Elliptic Curve defined by y^2 = x^3 + x + 6 over Finite Field of size 11
P = E(5, 2)

a = 2*P
b = 3*P
c = 4*P
d = 5*P
e = 6*P
f = 7*P
```

```
g = 8*P
h = 9*P
i = 10*P
j = 11*P
k = 12*P
l = 13*P


print P
print a
print b
print c
print d
print e
print f
print g
print h
print i
print j
print k
print l

#(5 : 2 : 1)
#(10 : 2 : 1)
#(7 : 9 : 1)
#(3 : 5 : 1)
#(8 : 8 : 1)
#(2 : 4 : 1)
#(2 : 7 : 1)
#(8 : 3 : 1)
#(3 : 6 : 1)
#(7 : 2 : 1)
#(10 : 9 : 1)
#(5 : 9 : 1)
#(0 : 1 : 0)
```

3.

We can use Hasse's Theorem to determine a range of possible orders for the elliptic curves defined under GF(p) using the following equation:

$p+1- 2\sqrt{p} \le \#E(GF(p)) \le p+1+ 2\sqrt{p}$

For GF(11), we have:

$12 – 2\sqrt{11} \le \#(GF(11)) \le 12 + 2\sqrt{11}$, which is approximately equal to: $5.366 \le \#(GF(11)) \le 18.633$

We already know this is true, as, with the previous problem, the cardinality of the elliptic curve on GF(11) is 13.

Because 13 is a prime number, the only possible orders of the groups generated are 1 and 13. Each of the elements generates more than 1 (and so has to generate 13 elements). Thus, all elements are generators (primitive elements).

4.

a.

```
β = α
for(0;n-1, n++);
  β = elldouble(α)
  if(nextbit.equals() 1)
        β = elladd(α)
```

b.

$19 = (10011)_2$

β = α (1)

β = elldouble(β) (10)

NOP

β = elldouble(β) (100)

NOP

β = elldouble(β) (1000)

β = elladd(β) (1001)

β = elldouble(β) (10010)

β = elladd(β) (10011)

$160 = (10100000)_2$

β = α (1)

β = elldouble(β) (10)

NOP

β = elldouble(β) (100)

β = elladd(β) (101)

β = elldouble(β) (1010)

NOP

β = elldouble(β) (10100)

NOP

β = elldouble(β) (101000)
NOP
β = elldouble(β) (1010000)
NOP
β = elldouble(β) (10100000)

c.
We will require n/2 – 1 point additions, and n-- 1 doublings
d.
One double and add: $(20*10^{-6})(n/2-1 + n-1) = (20*10^{-6})*(79 + 159) = 4.76$ ms
For Menezes-Vanstone encryption,
the throughput will be:

5.
a. So, we have the elliptic curve $y^2 = x^3 + x + 13$ over Z_{31}. #E = 34, and (9, 10) is an element of order 34. Bob's secret exponent a = 25.
a. We need to compute β = aα.
β = 25*(9, 10)
We can do point doubling to obtain 2*(9, 10), then 4*(9, 10), and so on until we have 16*(9, 10) + 8*(9, 10) + (9, 10) to obtain 25*P = β.
Computing this similarly as in 4 using sage, we find β = 25*(9, 10) = (16, 23)
b.
Next, we decrypt this:
((4; 9); 28; 7); ((19; 28); 9; 13); ((5; 22); 20; 17); ((25; 16); 12; 27)

First with:
((4; 9); 28; 7);
We take C = aR = 25*(4, 9) = (18, 29) [obtained with sage]
So what we do here is compute m_1 and m_2 using the equation $m_i = c_i^{-1}*y_i \bmod 31$, where $y_1 = 28$, and $y_2 = 7$.
So $m_1 = 18^{-1}*28 \bmod 31 = 19*28 \bmod 31 = 5$
and $m_2 = 29^{-1}*7 \bmod 31 = 15*7 \bmod 31 = 12$
Continuing from here:
((19; 28); 9; 13);
C = 25*(19, 28) = (24, 29)
Then, $m_1 = 24^{-1}*28 \bmod 31 = 12$
and $m_2 = 29^{-1}*7 \bmod 31 = 9$

Next:
((5; 22); 20; 17);
C = aR = 25*(5, 22) = (9, 21)
$m_1 = 9^{-1}$*20 mod 31 =140 mod 31 = 16
$m_2 = 21^{-1}$*17 mod 31 = 51 mod 31 = 20
Lastly, we determine:
((25; 16); 12; 27)
Again, using sage, we find that:
$(c_1, c_2) = (22, 9)$
$m_1 = 22^{-1}$ * 13 mod 31 = 24*12 mod 31 = 9
$m_2 = 9^{-1}$ * 27 mod 31 = 3
So our combined results are: 5, 12, 12, 9, 16, 20, 9, 3

c.
Converting these using the scale provided:
5 => E
12 => L
12 => L
9 => I
16 => P
20 => T
9 => I
3 => C
Our plaintext is “Elliptic.”

6. Taking $y = \lambda x + b$, and then inserting this into the elliptic curve equation of $y^2 = x^3 + ax + b \rightarrow$
$(\lambda x + c)^2 = x^3\ ax + b \rightarrow$
$\lambda^2 x^2 + 2\lambda xc + c^2 = x^3 + ax + b \rightarrow$
$x^{3\,-}\lambda^2 x^2 - 2\lambda xc +- ax + b - c^2 \rightarrow$
$x^{3\,-}\lambda^2 x^2 + x*(a - 2\lambda c) + b - c^2 \rightarrow$
Knowing that $x_0 + x_1 + x_2 = -a_2 = \lambda^2$,
$x^{3\,-}\lambda^2 x^2 + x*(a - 2\lambda c) + b - c^2 = (x_0)x^3 - (x_0 + x_1 + x_2)x^2 + (x_0x_1 + x_0x_2 + x_1x_2)x - x_0x_1x_2$
$^{-}\lambda^{2\,=} x_0 + x_1 + x_2$
$a - 2\lambda c = x_0x_1 + x_0x_2 + x_1x_2$
$x^{3\,-}\lambda^2 x^2 + x*(a - 2\lambda c) + b - c^2 = (x_0)x^3 - (x_0 + x_1 + x_2)x^2 + (x_0x_1 + x_0x_2 + x_1x_2)x - x_0x_1x_2$
So $\lambda^{2\,=\,-}x_0 + -x_1 + -x_2$
$x_2 = -\lambda^2 + x_0 + x_1$
So we have $x_R = \lambda^2 - x_P - x_Q$ for $x_2 = x_R$, $x_1 = x_P$ and $x_0 = x_Q$.
Then, to compute the value for y_R,
$y_0 = \lambda x_0 + c$
$y_2 = -(\lambda x_2 + y_1 - \lambda x_1) = -(\lambda(x_2 - x_1) + y_1) = y_R$