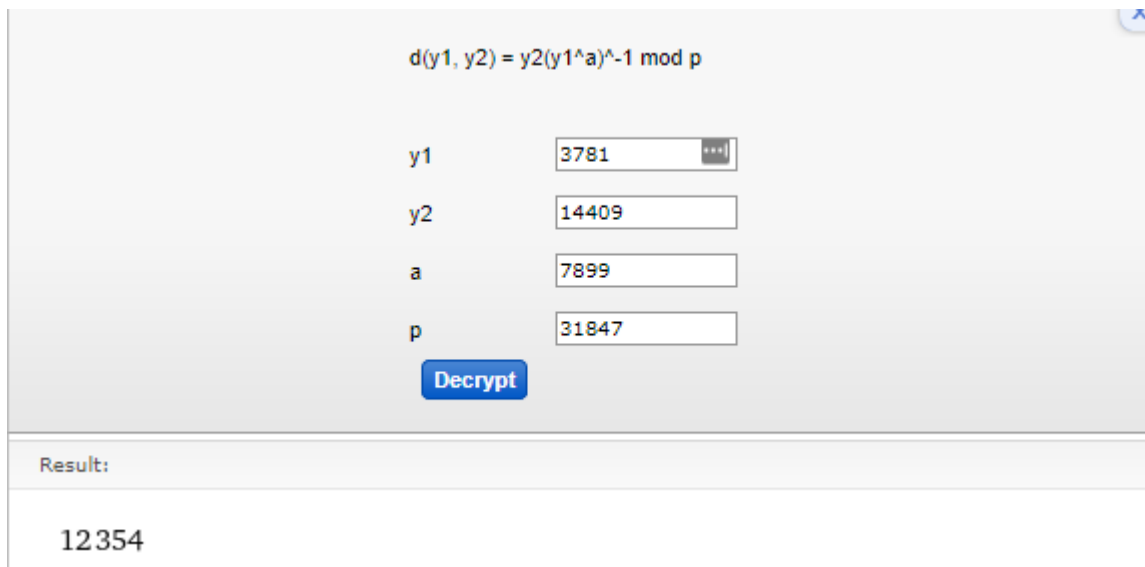


7.9

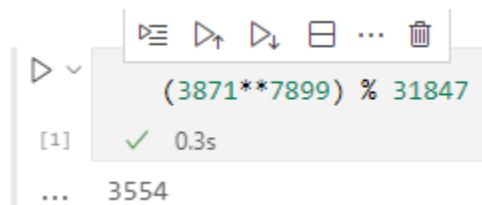
I couldn't figure this problem out. It seemed simple, where I thought I would just have to plug the pairs into the *elgamal*d function on the V200, using a pair as my y , then p and a as in the book. I tried plugging that into a WolframAlpha ElGamal Decryptor widget (<https://www.wolframalpha.com/widgets/view.jsp?id=978d7097ff2a699194ad4282bd27b1dc>), but when I tried to do the method myself, I got 28885 instead of 12354.



The screenshot shows a web interface for an ElGamal Decryptor. At the top, the formula $d(y1, y2) = y2(y1^a)^{-1} \bmod p$ is displayed. Below the formula are four input fields: $y1$ with the value 3781, $y2$ with the value 14409, a with the value 7899, and p with the value 31847. A blue button labeled "Decrypt" is positioned below the input fields. At the bottom of the interface, under the heading "Result:", the output value 12354 is displayed.

Figure 1

My process involved using the formula on the top of *Figure 1*. I first did my $y1^a$, which was 31847^{7899} . I took this mod p to make it manageable, which left me with



The screenshot shows a code editor with a toolbar at the top containing icons for running, stepping through, and other execution controls. The code entered is $(3871^{**}7899) \% 31847$. Below the code, the execution result is shown as $[1] \quad \checkmark \quad 0.3s \quad \dots \quad 3554$, indicating that the calculation completed successfully and returned the value 3554.

Figure 2

Then, I used my program that I've added to a previous assignment that finds *all* the invertible elements and their inverses, given a modulus. I searched this table for 3554, and found the inverse, which I then multiplied by $y2 \bmod p$.

3552		3550	4638
3553		3551	4834
3554		3552	11844
3555		3553	735
3556		3554	21766
3557		3555	10544
3558		3556	4057
3559		3557	1343
3560		3558	546
3561		3559	12635

Figure 3

$21766 \times 14409 \bmod 31847 = 28885$.

This is also the answer I got when I plugged in the following into the V200:

$[[3871][14409]] \rightarrow y$

$31847 \rightarrow p$

$7899 \rightarrow a$

$elgamald(y, p, a)$

output: 28885

However, this differs from the computed value from above, and I can't figure out how to get to the correct answer.

7.10

I tried to follow this top answer's guide to find these polynomials:

<https://math.stackexchange.com/questions/32197/find-all-irreducible-monic-polynomials-in-mathbbz-2x-with-degree-equal>

However, I had a hard time following, so I fully just checked the problems against his list.

$$x^5 + x^4 + 1 - \text{Reducible}$$

$$x^5 + x^3 + 1 - \text{Irreducible}$$

$$x^5 + x^4 + x^2 + 1 - \text{Reducible}$$

7.12

I tried setting up the problem as in **7.9**:

$$(K, H) \rightarrow y$$

$$K, H = 2x + 2, x^2 + 2$$

$$y^2 (y^{1^a})^{-1} \bmod p$$

$$x^2 + 2 \left((2x + 2)^{11} \right)^{-1} \bmod p$$

However, this seemed impossible to solve without a proper value for p , and I had no idea where to go next.

I apologize for the poor workmanship on this and the past few assignments. I got married this past Saturday, and I've had no time for anything else.