Dennis Kuzminer
CSCI-UA 310-001 PS4

1. ExtEuclid(117, 67) →

i	0	1	2	3	4	5
a_i	117	67	50	17	16	1
b_i	67	50	17	16	1	0
s_i	-4	3	-1	1	0	1
t_i	7	-4	1	-1	1	0
q_i	1	1	2	1	16	

$d = 1$

$s = -4$

$t = 7$

$as + bt = d \rightarrow 117(-4) + 67(7) = 1$

Dennis Kuzminer
CSCI-UA 310-001 PS4

2. Exercise 1.10. Show that if $a \geq b > 0$, then the values s and t computed by ExtEuclid(a, b) satisfy

$$|s| \leq b/d \quad \text{and} \quad |t| \leq a/d.$$

Hint: prove by induction on b—be careful, you have to stop the induction before b gets to zero, so the last step to consider is when $b \mid a$.

Base case: b divides a is the base case

$s, \ t \ = 0$ $\rightarrow$ By definition b and a are greater than 0. This means that d = gcd(a, b) must be at least 1. This implies that b/d and a/d must be a least one as well. Therefore, $|s| \leq b/d, \ |t| \leq a/d$ hold when $s, \ t \ = 0$

s<b/d, t<a/d , s=t'

a'/d'<b/d

D never changes so we can cancel out d

A' < b

Inductive step: assume it works for ext(b,a mod b) (ext(e,f)) then prove that it works for ext(a,b)

Base case: $b|a, \ s = 0, \ t = 1, \ d = b \rightarrow |s| \leq b/d, \ |t| \leq a/d$ both hold.

Inductive step: Assume that the condition holds for ExtEuclid(b, r), r = a mod b

This means that gcd(b, r) implies $\rightarrow$ gcd(a, b). This is because gcd(b, r), gcd(a, b) = d, showing that d will be invariant.

We can also see that $s = t', \ t = s' - qt'$

Dennis Kuzminer
CSCI-UA 310-001 PS4

3.

a. If b/d and a/d are relatively prime, this implies that $gcd(b/d,\ a/d)\ = 1$. If b/d and a/d are not relatively prime, meaning that $gcd(b/d,\ a/d)\ \neq 1$, then $gcd(b,\ a)\ \neq d$, as there will always be some number $(gcd(b,\ a)\ > d)$ larger than d that would be the real gcd. This number will continue to become larger until it satisfies the condition that $gcd(b,\ a)\ = d,\ gcd(b/d,\ a/d)\ = 1$.
More formally,
By Bezout's Lemma, we know $as + bt = d \rightarrow (a/d)s + (b/d)t = 1$. We can rewrite the equation setting $a' = (a/d),\ b' = (b/d) \rightarrow a's + b't = 1$. By Theorem 1.7 (Corollary to Bezout's Lemma), we can see that $a',\ b'$ are both relatively prime.

b. We can apply similar logic to show that s and t are relatively prime.
By Bezout's Lemma, we know $as + bt = d \rightarrow (a/d)s + (b/d)t = 1$. We can rewrite the equation setting $s' = (a/d),\ t' = (b/d),\ a' = s,\ b' = t \rightarrow a's' + b't' = 1$. By Theorem 1.7 (Corollary to Bezout's Lemma), we can see that $a',\ b'$ are both relatively prime, meaning that both s and t are relatively prime.

Dennis Kuzminer
CSCI-UA 310-001 PS4

4. $a|n,\ b|n,\ gcd(a,b) = 1 \rightarrow$ Prove $ab|n$
   By Bezout's Lemma,
   $as + bt = 1$ for some $s, t \in \mathbb{Z}$ $\rightarrow$ Multiply by n $\rightarrow$ $asn + btn = n$
   We can say that $n = bk,\ n = aj$ for some $k, j \in \mathbb{Z}$, as n|a, b
   $bkas + ajbt = n \rightarrow ab(ks + jt) = n \rightarrow$
   $(ks + jt) \in \mathbb{Z}$. This means that ab|n.

Dennis Kuzminer
CSCI-UA 310-001 PS4

5. Let i be a bit's place/index such that $i \in \{0, ...\ n-1\}$. If $\widehat{x}$ is the complement of x, such that if $\widehat{x}_i = 0$ then $x_i = 1$ and if $\widehat{x}_i = 1$ then $x_i = 0$, we can add each digit of place/index i to see a relationship between the two numbers. Because $\widehat{x}_i$ and x_i will always be opposite their bit sum will always be 1 + 0 = 1. Therefore, for each place i, $\widehat{x}_i + x_i = 1$. More specifically, this also shows that for $i \in \{0, ...\ n-1\}$, $\widehat{x} + x = 1_{2^{n-1}} \dots 1_{2^2}\ 1_{2^1}\ 1_{2^0} \rightarrow \widehat{x} + x = 1$ (repeated n times).
   This implies that $\widehat{x} + x = 2^n - 1 \rightarrow \widehat{x} + 1 = 2^n - x$
   We know that $x + ny \equiv x(mod\ n),\ y \in \mathbb{Z} \rightarrow 2^n - x \equiv - x(mod\ 2^n) \rightarrow \widehat{x} + 1 \equiv - x(mod\ 2^n)$

Dennis Kuzminer
CSCI-UA 310-001 PS4

6.

a. $100z + 200 \equiv 93z + 171 \ (mod\ 1000) \rightarrow 7z \equiv -29 \ (mod\ 1000) \rightarrow 7z \equiv 971 (mod\ 1000)$
$d = gcd(7, 1000) = 1 \rightarrow$ There is a unique solution from [1...n).
$z = 971t\ mod\ 1000,\ t = 7^{-1} mod\ 1000 \rightarrow$ ExtEuclid(1000, 7) $\rightarrow d = 1,\ s = -1,\ t = 143$
$z = 29(143)\ mod\ 1000 \rightarrow 4147\ mod\ 1000 =$ **853**

b. $115z + 130 \equiv 100z + 165 \ (mod\ 1000) \rightarrow 15z \equiv 35 \ (mod\ 1000) \rightarrow d = gcd(a, n) \rightarrow$
$d = gcd(15, 1000) = 5 \rightarrow$ There are unique solutions from [1...n), as 5|35.
$15z \equiv 35 \ (mod\ 1000) \rightarrow /d \rightarrow 3z \equiv 7 \ (mod\ 200)$
$z = 7t\ mod\ 200,\ t = 15^{-1} mod\ 1000 \rightarrow$ ExtEuclid(1000, 15) $\rightarrow d = 5,\ s = -1,\ t = 67$
$z = 469\ mod\ 200 = 69 \rightarrow$ Other solutions: 69+0, 69+200, 69+4(200), 69+2(200), 69+3(200) → **69, 269, 469, 669, 869**

c. $115z + 132 \equiv 100z + 140 \ (mod\ 1000) \rightarrow 15z \equiv 8 \ (mod\ 1000) \rightarrow d = gcd(a, n) \rightarrow$
$d = gcd(15, 1000) = 5 \rightarrow$ There are **no solutions** in [1...n), as 5∤8.

d. $119z + 132 \equiv 113z + 140 \ (mod\ 1000) \rightarrow 6z \equiv 8 \ (mod\ 1000) \rightarrow d = gcd(a, n) \rightarrow$
$d = gcd(6, 1000) = 2 \rightarrow$ There are unique solutions from [1...n), as 2|8.
$6z \equiv 8 \ (mod\ 1000) \rightarrow /d \rightarrow 3z \equiv 4 \ (mod\ 500)$
$z = 4t\ mod\ 500,\ t = 6^{-1} mod\ 1000 \rightarrow$ ExtEuclid(1000, 6) $\rightarrow d = 2,\ s = -1,\ t = 167$
$z = 4(167)\ mod\ 500 \rightarrow 668\ mod\ 500 = 168 \rightarrow$ Other solutions: 168+0, 168+500 → **168, 668**

Dennis Kuzminer
CSCI-UA 310-001 PS4

7.

i	1	2	3	4	5	6	7	8	9	10	11	12...
9^i mod 100	9	81	29	61	49	41	69	21	89	1	9	81...

Order: 10

From the table, we can see that $9^9 * 9 \; mod \; 100$ gives 1. This implies that **89** is the multiplicative inverse of $9 \; mod \; 100$. This is because multiplying this by 9 once more gives 1.

Dennis Kuzminer
CSCI-UA 310-001 PS4

8. By modular multiplication, we know that $(A * B)\ mod\ C = (A\ mod\ C * B\ mod\ C)\ mod\ C$.
Therefore, $3^{99}\ mod\ 100$ can be shown as
((some combination of numbers that multiply to 3^{99}) $each\ mod\ 100)\ mod\ 100$.
We can have the combination of numbers be powers of 2 using base 2 and the repeated squaring algorithm.
$e = 99_{10} = 1100011_2$
$\beta \leftarrow [1]$ // 0
$\beta \leftarrow \beta^2,\ \beta \leftarrow \beta * \alpha$ //1 $\rightarrow 3^1\ mod\ 100 = 3$
$\beta \leftarrow \beta^2,\ \beta \leftarrow \beta * \alpha$ //11 $\rightarrow 3^3\ mod\ 100 = 27$
$\beta \leftarrow \beta^2$ //110 $\rightarrow 3^6\ mod\ 100 = 27^2\ mod\ 100 = 29$
$\beta \leftarrow \beta^2$ //1100 $\rightarrow 3^{12}\ mod\ 100 = 29^2 mod\ 100 = 41$
$\beta \leftarrow \beta^2$ //11000 $\rightarrow 3^{24}\ mod\ 100 = 41^2 mod\ 100 = 81$
$\beta \leftarrow \beta^2,\ \beta \leftarrow \beta * \alpha$ //110001 $\rightarrow 3^{49}\ mod\ 100 = 81^2 mod\ 100 * 3 = 83$
$\beta \leftarrow \beta^2,\ \beta \leftarrow \beta * \alpha$ //1100011 $\rightarrow 3^{99}\ mod\ 100 = 83^2 mod\ 100 * 3 =$ **67**

Dennis Kuzminer
CSCI-UA 310-001 PS4

9. $gh = ([2]x^2 + [3]x + [4])([3]x^2 + [2]x + [1]) \rightarrow$

$[2][3]x^4 + [2][2]x^3 + [2][1]x^2 + [3][3]x^3 + [3][2]x^2 + [3][1]x + [4][3]x^2 + [2][4]x + [4][1] \rightarrow$

$[1]x^4 + [4]x^3 + [2]x^2 + [4]x^3 + [1]x^2 + [3]x + [2]x^2 + [3]x + [4] \rightarrow$

$[1]x^4 + [3]x^3 + [0]x^2 + [1]x + [4] \rightarrow$

$[1]x^4 + [3]x^3 + [0]x^2 + [1]x + [4]$ *mod* $x^3 + x + [1] \rightarrow$

$$
\begin{array}{r|l}
 & x + [3] \\
\hline
x^3 + x + [1] & x^4 + [3]x^3 + [0]x^2 + x + [4] \\
 & \underline{-x^4 - [0]x^3 - x^2 - x \quad \downarrow} \\
 & [3]x^3 + [4]x^2 + [0]x + [4] \\
 & \underline{-[3]x^3 - [0]x^2 - [3]x - [3]} \\
 & [4]x^2 + [2]x + [1]
\end{array}
$$

$\checkmark$

$gh \bmod f = [4]x^2 + [2]x + [1]$

Dennis Kuzminer
CSCI-UA 310-001 PS4

10. $u_1 = [1],\ u_2 = [2],\ u_3 = [3]\ ,\ v_1 = [3],\ v_2 = [4],\ v_3 = [1]$

$$g([x]) = [3]\frac{(x-[2])(x-[3])}{([1]-[2])([1]-[3])} + [4]\frac{(x-[1])(x-[3])}{([2]-[1])([2]-[3])} + [1]\frac{(x-[1])(x-[2])}{([3]-[1])([3]-[2])} \rightarrow$$

$$[3]\frac{x^2+[0]x+[1]}{([1]-[2])([1]-[3])} + [4]\frac{x^2+[1]x+[3]}{([2]-[1])([2]-[3])} + [1]\frac{x^2+[2]x+[2]}{([3]-[1])([3]-[2])} \rightarrow$$

$$[3]\frac{x^2+[0]x+[1]}{([4])(3])} + [4]\frac{x^2+[1]x+[3]}{([1])([4])} + [1]\frac{x^2+[2]x+[2]}{([2])([1])} \rightarrow$$

$$[3]\frac{x^2+[0]x+[1]}{[2]} + [4]\frac{x^2+[1]x+[3]}{[4]} + [1]\frac{x^2+[2]x+[2]}{[2]} \rightarrow$$

$$[3][3](x^2 + [0]x + [1]) + [4][4](x^2 + [1]x + [3]) + [1][3](x^2 + [2]x + [2]) \rightarrow$$

$$[4](x^2 + [0]x + [1]) + [1](x^2 + [1]x + [3]) + [3](x^2 + [2]x + [2]) \rightarrow$$

$$[4]x^2 + [0]x + [4] + [1]x^2 + [1]x + [3] + [3]x^2 + [1]x + [1] \rightarrow$$

$$[3]x^2 + [2]x + [3] = g([x])$$

https://math.stackexchange.com/questions/1754541/confusion-about-elements-in-fields-like-1-in-z5
http://faculty.bard.edu/belk/math332/AlgebraicStructures.pdf