Prime Finite Fields (1)

- Earlier we showed that, in general, Z_n is a ***commutative ring***.
- The main reason for why, in general, Z_n is only a commutative ring and not a finite field is because ***not*** every element in Z_n is guaranteed to have a multiplicative inverse.
- In particular, as shown before, an element a of Z_n does not have a multiplicative inverse if a is ***not relatively prime*** to the modulus n.

Prime Finite Fields (2)

- What if we choose the modulus n to be a ***prime number***? (A prime number has only two divisors, one and itself.)

- For ***prime*** n, every element $a \in Z_n$ will be relatively prime to n. That implies that there will exist a multiplicative inverse for every $a \in Z_n$ for prime n.

- Therefore, $\boldsymbol{Z_p}$ is a finite field if we assume p denotes a prime number. Z_p is sometimes referred to as a ***prime finite field***. Such a field is also denoted ***GF (p)***, where *GF* stands for "Galois Field".

What Happened to the Main Reason for Why Z_n Could not be an Integral Domain? (1)

- Earlier, when we were looking at how to characterize Z_n, we said that, although it possessed a multiplicative identity, it could not be an integral domain because Z_n allowed for the equality $a \times b = 0$ even for non-zero a and b. (Recall, 0 means the additive identity element.)
- If we have now decided that Z_p is a *finite field* for prime p because every element in Z_p has a unique multiplicative inverse, are we sure that we can now also guarantee that if $a \times b = 0$ then either a or b must be 0?

What Happened to the Main Reason for Why Z_n Could not be an Integral Domain? (2)

- Yes, *we have that guarantee* because $a \times b = 0$ for general Z_n occurs only when non-zero a and b are factors of the modulus n. When n is a prime, its only factors are 1 and n. So with the elements of Z_n being in the range 0 through $n - 1$, the only time we will see $a \times b = 0$ is when either a is 0 or b is 0.

Finding Multiplicative Inverses for Elements of Z_p (1)

- In general, to find the multiplicative inverse of $a \in Z_n$, we need to find the element b such that

$$a \times b = 1 \; mod \; n$$

- Based on the discussion so far, we can say that the multiplicative inverses exist for all $a \in Z_n$ for which we have

$$gcd\,(a, n) = 1$$

- Obviously, when n equals a prime p, this condition will always ***be satisfied by all elements*** of Z_p.

Finding Multiplicative Inverses for Elements of Z_p (2)

- In general, it can be shown that when a and n are any pair of positive integers, the following must always hold for some integers x and y (that may be positive or negative or zero):

$$gcd\,(a, n) = x \times a + y \times n$$

- This is known as the ***Bezout's Identity***.
- For example, when $a = 16$ and $n = 6$, we have $gcd\,(16, 6) = 2$. We can certainly write: $2 = (-1) \times 16 + 3 \times 6 = 2 \times 16 + (-5) \times 6$. This shows that x and y *do not have to be unique* in Bezout's identity for given a and n.

Finding Multiplicative Inverses Using Bezout's Identity (1)

- Given an a that is relatively prime to n, we must obviously have $gcd\,(a, n) = 1$. Such an a and n must satisfy the following constraint for some x and y:

$$x \times a + y \times n = 1$$

- Let's now consider this equation modulo n. Since y is an integer, obviously $y \times n \bmod n$ equals 0. Thus, it must be the case that, considered modulo n, x equals a^{-1}, the multiplicative inverse of a modulo n.
- The equation shown above gives us a ***strategy*** for finding the multiplicative inverse of an element a :

Finding Multiplicative Inverses Using Bezout's Identity (2)

This strategy is:

1. We use the same Euclid algorithm as before to find the $gcd\,(a, n)$,
2. but now at each step we write the expression in the form $a \times x + n \times y$ for the remainder
3. eventually, before we get to the remainder becoming 0, when the remainder becomes 1 (which will happen only when a and n are relatively prime), x will automatically be the multiplicative inverse we are looking for.

The Extended Euclid's Algorithm for Calculating the Multiplicative Inverse (1)

- So our quest for finding the ***multiplicative inverse (MI)*** of a number *num* modulo *mod* boils down to expressing the residues at each step of Euclid's recursion as a linear sum of *num* and *mod*, and, when the recursion terminates, taking for ***MI*** the coefficient of *num* in the final linear summation.
- As we step through the recursion called for by Euclid's algorithm, the originally supplied values for *num* and *mod* become modified as shown earlier. So let's use *NUM* to refer to the originally supplied value for *num* and *MOD* to refer to the originally supplied value for *mod*.

The Extended Euclid's Algorithm for Calculating the Multiplicative Inverse (2)

- Let x represent the coefficient of NUM and y the coefficient of MOD in our linear summation expressions for the residue at each step in the recursion. So our goal is to express the residue at each step in the form

$$residue = x * NUM + y * MOD$$

- And then, when the *residue* is 1, to take the value of x as the multiplicative inverse of NUM modulo MOD, assuming, the MI exists.

The Extended Euclid's Algorithm for Calculating the Multiplicative Inverse (3)

What is interesting is that as the Euclid's recursion proceeds, the new values of x and y can be computed directly from their current values and their previous values (which we will denote x_{old} and y_{old}) by the formulas:

$$x <= x_{old} + x * q$$

$$y <= y_{old} + y * q$$

where q is the integer quotient obtained by dividing *num* by *mod*. To establish this fact, the following table in the next page illustrates an example for calculating *gcd* (17, 32) where we are interested in finding the ***MI*** of 17 modulo 32:

The Extended Euclid's Algorithm for Calculating the Multiplicative Inverse (4)

Row	q = num//mod	num	mod	x	y
A. Initialization				1	0
B.		17	32	0	1
C. gcd(17, 32)					
D. residue = 17	17//32 = 0	32	17	1	0
E. gcd(32, 17)					
F. residue = 15	32//17 = 1	17	15	-1	1
G. gcd(17, 15)					
H. residue = 2	17//15 = 1	15	2	2	-1
I. gcd(15, 2)					
J. residue = 1	15//2 = 7	2	1	-15	8

Rules for Table Construction in the Extended Euclid's Algorithm (1)

1. Rows A and B of the table are for ***initialization***. We set x_{old} and y_{old} to 1 and 0, respectively, and their current values to 0 and 1. At this point, *num* is 17 and *mod* 32.

2. Note that the ***first thing*** we do in each new row is to calculate the ***quotient*** obtained by dividing the current *num* by the current *mod*.

3. ***Only after that*** we ***update the values*** of *num* and *mod* in that row according to Euclid's recursion.

Rules for Table Construction in the Extended Euclid's Algorithm (2)

- For example, when we calculate *q* in row F, the current *num* is 32 and the current *mod* 17. Since the integer quotient obtained when you divide 32 by 17 is 1, the value of *q* in this row is 1.

- Having obtained the ***residue***, we now invoke ***Euclid's recursion***, which causes *num* to become 17 and *mod* to become 15 in row F.

4. We *update* the ***values of x*** on the basis of its current value and its previous value and the current value of the quotient *q*

Rules for Table Construction in the Extended Euclid's Algorithm (3)

- For example, when we calculate the value of x in row J, the current value for x at that point is the one shown in row H, which is 2, and the previous value for x is shown in row F, which is -1. Since the current value for the quotient q is 7, we obtain the new value of x in row J by $-1 - 7 * 2 = -15$. This is according to the update formula for the x coefficients:

$$x_{\text{new}} = x_{old} - q \times x_{\text{current}}$$

5. The same goes for the ***variable y*** . It is ***updated*** in the same manner through the formula

$$y_{\text{new}} = y_{old} - q \times y_{\text{current}}$$

Finally . . .

- **Acknowledgment:** These lecture notes are based on the textbook by William Stallings and notes prepared by Avinash Kak, Purdue University. My sincere thanks are devoted to them and to all other people who offered the material on the web.
- Students are advised to study and solve the problems and answer the questions in **Assignment-6**.
- Students are encouraged to read more about the details of the ***Hill cipher*** in the supplied ***tutorial***.