Z_{26} (The Integers mod 26)

An element x of Z_n has an *inverse* in Z_n if there is an element y in Z_n such that $xy \equiv 1 \pmod{n}$. When x has an inverse, we say x is *invertible*. When $xy \equiv 1 \pmod{n}$, we call y the *inverse* of x, and write $y = x^{-1}$. Note $y = x^{-1}$ implies $x = y^{-1}$, and hence y is also invertible.

Since $xy \equiv 1 \pmod{n}$ is equivalent to $(-x)(-y) \equiv 1 \pmod{n}$, we can say that if x is invertible with $x^{-1} = y$, then $-x$ is invertible $(-x)^{-1} = -y$. Also, for any integer k, $xy \equiv 1 \pmod{n}$ implies $x^k y^k \equiv (xy)^k \equiv 1^k \equiv 1 \pmod{n}$, which tells us that x^k is invertible and $(x^k)^{-1} = (x^{-1})^k$

We will prove shortly that x has an inverse in Z_n if and only if $gcd(x,n) = 1$. In fact, the proof will be constructive; it will give us an effective algorithm for computing the inverse when it exists. If n is prime, then every nonzero element of Z_n has an inverse. However, if n is composite, there are fewer invertible elements. We define $\varphi(n)$ to be the number of elements of $\{1,2, \ldots, n-1\}$ that are relatively prime to n, i.e., the number of invertible elements of Z_n. If we can factor n, we can find $\varphi(n)$.[1] Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the factorization of n as a product of powers of distinct primes. Then

$$\varphi(n) = n(1-1/p_1)(1-1/p_2)(1-1/p_r).$$

In the special case that $e_1 = e_2 = \ldots = e_r = 1$, the formula for $\varphi(n)$ simplifies to

$$\varphi(n) = (p_1-1)(p_2-1) \ldots (p_r-1).$$

We specialize to the case $n = 26 = 2 \cdot 13$. $\varphi(26) = (2-1)(13-1) = 12$. The twelve invertible elements of Z_{26} are:

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

The table of inverses is

Inverses mod 26												
x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Here is the complete multiplication table for Z_{26}. Note the table of inverses follows from the positions of the 1s in this table.

[1] Conversely, if we can compute $\varphi(n)$, then we can factor n, at least in the special case that n is the product of two primes. This will turn out to be critical when we look at the RSA algorithm.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

We can obtain all the invertible elements of Z_{26} as powers of some single invertible element.

Powers of 7 (mod 26)												
k	1	2	3	4	5	6	7	8	9	10	11	12
7^k (mod 26)	7	23	5	9	11	25	19	3	21	17	15	1

(We could have used 11, 19, or 15 in place of 7.) This property does not hold in Z_n for arbitrary n. It holds $n = p^e$ or $n = 2p^e$, where p is an odd prime and e is arbitrary. However, it is always true (for any n) that x invertible implies $x^{\varphi(n)} \equiv 1 \pmod{n}$.