

Ring	k											
	1	2	3	4	5	6	7	8	9	10	11	12
\mathbb{Z}_{11}	[2]	[4]	[8]	[5]	[10]	[9]	[7]	[3]	[6]	[1]		
	[3]	[9]	[5]	[4]	[1]							
	[4]	[5]	[9]	[3]	[1]							
	[5]	[3]	[4]	[9]	[1]							
	[6]	[3]	[7]	[9]	[10]	[5]	[8]	[4]	[2]	[1]		
	[7]	[5]	[2]	[3]	[10]	[4]	[6]	[9]	[8]	[1]		
	[8]	[9]	[6]	[4]	[10]	[3]	[2]	[5]	[7]	[1]		
	[9]	[4]	[3]	[5]	[1]							
	[10]	[1]										
	\mathbb{Z}_{12}	[2]	[4]	[8]	[4]*							
[3]		[9]	[3]*									
[4]		[4]*										
[5]		[1]										
[6]		[0]	[0]*									
[7]		[1]										
[8]		[4]	[8]*									
[9]		[9]*										
[10]		[4]	[4]*									
[11]		[1]										
\mathbb{Z}_{13}	[2]	[4]	[8]	[3]	[6]	[12]	[11]	[9]	[5]	[10]	[7]	[1]
	[3]	[9]	[1]									
	[4]	[3]	[12]	[9]	[10]	[1]						
	[5]	[12]	[8]	[1]								
	[6]	[10]	[8]	[9]	[2]	[12]	[7]	[3]	[5]	[4]	[11]	[1]
	[7]	[10]	[5]	[9]	[11]	[12]	[6]	[3]	[8]	[4]	[2]	[1]
	[8]	[12]	[5]	[1]								
	[9]	[3]	[1]									
	[10]	[9]	[12]	[3]	[4]	[1]						
	[11]	[4]	[5]	[3]	[7]	[12]	[2]	[9]	[8]	[10]	[6]	[1]
	[12]	[1]										

Problem 32:

(a) The congruence classes whose lines end with | in the above table, as well as [1], have some power that is [1]. Effectively these are:

In \mathbb{Z}_2 : [1] (all non-zero classes)

In \mathbb{Z}_3 : [1], [2] (all non-zero classes)

In \mathbb{Z}_4 : [1], [3]

In \mathbb{Z}_5 : [1], [2], [3], [4] (all non-zero classes)

In \mathbb{Z}_6 : [1], [5]

In \mathbb{Z}_7 : [1], [2], [3], [4], [5], [6] (all non-zero classes)

In \mathbb{Z}_8 : [1], [3], [5], [7]

In \mathbb{Z}_9 : [1], [2], [4], [5], [7], [8]

In \mathbb{Z}_{10} : [1], [3], [7], [9]

In \mathbb{Z}_{11} : [1], [2], [3], [4], [5], [6], [7], [8], [9], [10] (all non-zero classes)

In \mathbb{Z}_{12} : [1], [5], [7], [11]

In \mathbb{Z}_{13} : [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12] (all non-zero classes)

Conjecture: These are those congruence classes that represent an invertible element (unit) in \mathbb{Z}_n . Equivalently, those [a] for which $(a, n) = 1$.

(partial) Proof: If $(a, n) \neq 1$, then [a] is not invertible, hence no power of [a] can be invertible,

and so cannot be [1] (which is of course invertible). — The converse is true, but you cannot be expected to see the proof yet.

(b) We find it is exactly for $n = 2, 3, 5, 7, 11, 13$, that all non-zero congruence classes have some power that is [1].

Conjecture: This happens exactly if n is prime.

(partial) Proof: If n is composite, then there are non-invertible classes, and none of their powers could be [1]. Conversely, if n is prime, then all non-zero classes are invertible. If we can trust the (yet unproved) converse in part (a), then we could conclude that they all have some power that is [1].

(c) The number of those $[a]$ that have some power that is [1] is, according to part (a), exactly the number of those $[a]$ that are invertible in \mathbb{Z}_n , namely there are $\varphi(n)$ of them.

(d) The periods that occur for powers of invertible congruence classes are:

n	2	3	4	5	6	7	8	9	10	11	12	13
periods	1	1, 2	1, 2	1, 2, 4	1, 2	1, 2, 3, 6	1, 2	1, 2, 3, 6	1, 2, 4	1, 2, 5, 10	1, 2	1, 2, 3, 4, 6, 12
$\varphi(n)$	1	2	2	4	2	6	4	6	4	10	4	12

(The period 1 occurs for the class [1], which is not listed in the table of pblm 31.)

Conjecture: The periods that occur for powers of invertible classes in \mathbb{Z}_n are divisors of $\varphi(n)$.

Proof: From Euler's theorem, we know that $[a]^{\varphi(n)} = [1]$ for invertible congruence classes $[a]$ in \mathbb{Z}_n . (In other words, $a^{\varphi(n)} \equiv 1 \pmod{n}$, if $(a, n) = 1$.) If $[a]^k = [1]$ for some other k , then we have $[a]^{x\varphi(n)+yk} = [1]$ for any choice of integers x, y . In particular we choose x, y such that $x\varphi(n) + yk = \gcd(\varphi(n), k)$ and conclude that $[a]^{\gcd(\varphi(n), k)} = [1]$ as well.

Now if we are asking for the *smallest* positive k such that $[a]^k = [1]$, then $\gcd(\varphi(n), k) \leq k$ (always true for the gcd) and also $\gcd(\varphi(n), k) \geq k$ (since k was the smallest exponent such that $[a]^k = [1]$). Hence $\gcd(\varphi(n), k) = k$, and therefore k divides $\varphi(n)$.

(e) included in parts (a)–(d). Only conjectures were required for homework. Some proofs were provided in class upon turn-in of hwk, some will be provided.