ANSWERS
Math 345
Homework 11
11/22/2017

Exercise 42. Recall, for an integer a with $\gcd(a, n) = 1$, the *order* of $a \pmod{n}$, written $|a|$ or $|a|_n$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We call a a *primitive root* (mod n) if $|a|_n = \phi(n)$.

(a) Compute the orders of a for $1 \leq a < n$ with $\gcd(a, n) = 1$, for $n = 4, 8$, and 13.

Answers. Computing $a^i \pmod{n}$:

$n = 4, \phi(n) = 2$

	1	2	order
1	1	1	1
3	3	1	2

$n = 8, \phi(n) = 4$

	1	2	3	4	order
1	1	1	1	1	1
3	3	1	3	1	2
5	5	1	5	1	2
7	7	1	7	1	2

$n = 13, \phi(n) = 12$

	1	2	3	4	5	6	7	8	9	10	11	12	order
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

□

(b) Define $\psi_n(k) = \#\{1 \le a < p \mid |a| = k\}$ (as in class). Compute $\psi_n(k)$ for $1 \le k \le \phi$ for $p = 13$ and $p = 37$ (use a computer to generate data).

Answer. By part (a), for $n = 13$, we have the following.

k	1	2	3	4	5	6	7	8	9	10	11	12
$\psi_{13}(k)$	1	1	2	2	0	2	0	0	0	0	0	4

For for $n = 13$, see the table below to compute

k	1	2	3	4	6	9	12	18	36	else
$\psi_{37}(k)$	1	1	2	2	2	6	4	6	12	0

n 37

	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	26	27	28	29	30	31	32	33	34	35	36
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1
3	3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1	3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1
4	4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1	4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1
5	5	25	14	33	17	11	18	16	6	30	2	10	13	28	29	34	22	36	32	12	23	4	20	26	19	21	31	7	35	27	24	9	8	3	15	1
6	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1
7	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1
8	8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1
9	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1
10	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1
11	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1
12	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1
13	13	21	14	34	35	11	32	9	6	4	15	10	19	25	29	7	17	36	24	16	23	3	2	26	5	28	31	33	22	27	18	12	8	30	20	1
14	14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1
15	15	3	8	9	24	27	35	7	31	21	19	26	20	4	23	12	32	36	22	34	29	28	13	10	2	30	6	16	18	11	17	33	14	25	5	1
16	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1
17	17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1
18	18	28	23	7	15	11	13	12	31	3	17	10	32	21	8	33	2	36	19	9	14	30	22	26	24	25	6	34	20	27	5	16	29	4	35	1
19	19	28	14	7	22	11	24	12	6	3	20	10	5	21	29	33	35	36	18	9	23	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
20	20	30	8	12	18	27	22	33	31	28	5	26	2	3	23	16	24	36	17	7	29	25	19	10	15	4	6	9	32	11	35	34	14	21	13	1
21	21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1	21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1
22	22	3	29	9	13	27	2	7	6	21	18	26	17	4	14	12	5	36	15	34	8	28	24	10	35	30	31	16	19	11	20	33	23	25	32	1
23	23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1
24	24	21	23	34	2	11	5	9	31	4	22	10	18	25	8	7	20	36	13	16	14	3	35	26	32	28	6	33	15	27	19	12	29	30	17	1
25	25	33	11	16	30	10	28	34	36	12	4	26	21	7	27	9	3	1	25	33	11	16	30	10	28	34	36	12	4	26	21	7	27	9	3	1
26	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1
27	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1
28	28	7	11	12	3	10	21	33	36	9	30	26	25	34	27	16	4	1	28	7	11	12	3	10	21	33	36	9	30	26	25	34	27	16	4	1
29	29	27	6	26	14	36	8	10	31	11	23	1	29	27	6	26	14	36	8	10	31	11	23	1	29	27	6	26	14	36	8	10	31	11	23	1
30	30	12	27	33	28	26	3	16	36	7	25	10	4	9	11	34	21	1	30	12	27	33	28	26	3	16	36	7	25	10	4	9	11	34	21	1
31	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1
32	32	25	23	33	20	11	19	16	31	30	35	10	24	28	8	34	15	36	5	12	14	4	17	26	18	21	6	7	2	27	13	9	29	3	22	1
33	33	16	10	34	12	26	7	9	1	33	16	10	34	12	26	7	9	1	33	16	10	34	12	26	7	9	1	33	16	10	34	12	26	7	9	1
34	34	9	10	7	16	26	33	12	1	34	9	10	7	16	26	33	12	1	34	9	10	7	16	26	33	12	1	34	9	10	7	16	26	33	12	1
35	35	4	29	16	5	27	20	34	6	25	24	26	22	30	14	9	19	36	2	33	8	21	32	10	17	3	31	12	13	11	15	7	23	28	18	1
36	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1

□

(c) Prove that if $k \nmid \phi(n)$, then $\psi_n(k) = 0$.

Proof. If a has order k, then $k | \phi(n)$. So if $k \nmid \phi(n)$, then there are 0 elements of order k. So $\psi_n(k) = 0$. □

(d) List the primitive roots modulo 13.
For each primitive root ξ, for which k is ξ^k also a primitive root (mod 13)?

Proof.

ξ	k s.t. ξ^k is primitive
2	$1, 5, 7, 11$
6	$1, 5, 7, 11$
7	$1, 5, 7, 11$
11	$1, 5, 7, 11$

□

(e) List the primitive roots modulo 37.
For each primitive root ξ, for which k is ξ^k also a primitive root? (mod 37)

Answer. See the table below. The primitive roots are $3, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32$, and 35, and for each root ξ, ξ^k is also a primitive root for $k = 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31$, and 35.

n 37

	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	26	27	28	29	30	31	32	33	34	35	36
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1
3	3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1	3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1
4	4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1	4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1
5	5	25	14	33	17	11	18	16	6	30	2	10	13	28	29	34	22	36	32	12	23	4	20	26	19	21	31	7	35	27	24	9	8	3	15	1
6	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1
7	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1
8	8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1
9	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1
10	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1
11	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1
12	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1
13	13	21	14	34	35	11	32	9	6	4	15	10	19	25	29	7	17	36	24	16	23	3	2	26	5	28	31	33	22	27	18	12	8	30	20	1
14	14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1
15	15	3	8	9	24	27	35	7	31	21	19	26	20	4	23	12	32	36	22	34	29	28	13	10	2	30	6	16	18	11	17	33	14	25	5	1
16	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1
17	17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1
18	18	28	23	7	15	11	13	12	31	3	17	10	32	21	8	33	2	36	19	9	14	30	22	26	24	25	6	34	20	27	5	16	29	4	35	1
19	19	28	14	7	22	11	24	12	6	3	20	10	5	21	29	33	35	36	18	9	23	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
20	20	30	8	12	18	27	22	33	31	28	5	26	2	3	23	16	24	36	17	7	29	25	19	10	15	4	6	9	32	11	35	34	14	21	13	1
21	21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1	21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1
22	22	3	29	9	13	27	2	7	6	21	18	26	17	4	14	12	5	36	15	34	8	28	24	10	35	30	31	16	19	11	20	33	23	25	32	1
23	23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1
24	24	21	23	34	2	11	5	9	31	4	22	10	18	25	8	7	20	36	13	16	14	3	35	26	32	28	6	33	15	27	19	12	29	30	17	1
25	25	33	11	16	30	10	28	34	36	12	4	26	21	7	27	9	3	1	25	33	11	16	30	10	28	34	36	12	4	26	21	7	27	9	3	1
26	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1	26	10	1
27	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1	27	26	36	10	11	1
28	28	7	11	12	3	10	21	33	36	9	30	26	25	34	27	16	4	1	28	7	11	12	3	10	21	33	36	9	30	26	25	34	27	16	4	1
29	29	27	6	26	14	36	8	10	31	11	23	1	29	27	6	26	14	36	8	10	31	11	23	1	29	27	6	26	14	36	8	10	31	11	23	1
30	30	12	27	33	28	26	3	16	36	7	25	10	4	9	11	34	21	1	30	12	27	33	28	26	3	16	36	7	25	10	4	9	11	34	21	1
31	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1	31	36	6	1
32	32	25	23	33	20	11	19	16	31	30	35	10	24	28	8	34	15	36	5	12	14	4	17	26	18	21	6	7	2	27	13	9	29	3	22	1
33	33	16	10	34	12	26	7	9	1	33	16	10	34	12	26	7	9	1	33	16	10	34	12	26	7	9	1	33	16	10	34	12	26	7	9	1
34	34	9	10	7	16	26	33	12	1	34	9	10	7	16	26	33	12	1	34	9	10	7	16	26	33	12	1	34	9	10	7	16	26	33	12	1
35	35	4	29	16	5	27	20	34	6	25	24	26	22	30	14	9	19	36	2	33	8	21	32	10	17	3	31	12	13	11	15	7	23	28	18	1
36	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1	36	1

□

(f) For each of $n = 8$, 10, and 12, answer the following: Are there any primitive roots modulo n? If so, list them. If not, what is the largest order occurring modulo n?

Answer. $n = 8$: no, the smallest order is 2.
$n = 10$: yes, 3 and 7 have order $\phi(10) = 4$.
$n = 12$: no, the smallest order is 2.

□

Exercise 43. A function $f(n)$ that satisfies the multiplication formula $f(mn) = f(m)f(n)$ for all numbers m and n with $\gcd(m,n) = 1$ is called a *multiplicative function*. For example, we have seen that Eulers phi function $\phi(n)$ is multiplicative and that $F(n) = \sum_{d|n} \phi(n)$ is multiplicative. Now suppose that $f(n)$ is any multiplicative function, and define a new function

$$g(n) = f(d_1) + f(d_2) + \cdots + f(d_r),$$

where $1 = d_1 < d_2 < \cdots < d_{r-1} < d_r = n$ are the divisors of n.

Prove that $g(n)$ is a multiplicative function.

Proof. If $\gcd(m,n) = 1$, and

$$\text{the divisors of } m \text{ are } a_1, \ldots, a_k,$$

and

$$\text{the divisors of } n \text{ are } b_1, \ldots, b_\ell,$$

then $\gcd(a_i, b_j) = 1$ for all i, j, and the divisors of mn are $a_i b_j$ for $i = 1, \ldots, k$ and $j = 1, \ldots, \ell$. So

$$\begin{aligned} g(mn) &= \sum_{\substack{i=1,\ldots,k \\ j=1,\ldots,\ell}} f(a_i b_j) = \sum_{\substack{i=1,\ldots,k \\ j=1,\ldots,\ell}} f(a_i) f(b_j) \\ &= \left(\sum_{i=1,\ldots,k} f(a_i) \right) \left(\sum_{j=1,\ldots,\ell} f(b_j) \right) = g(m)g(n). \end{aligned}$$

□

Exercise 44. Define $\lambda(n)$ by factoring n into a product of primes,

$$n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

with $p_1 < p_2 < \cdots < p_\ell$ prime, and then setting

$$\lambda(n) = (-1)^{k_1 + k_2 + \cdots + k_\ell}, \qquad \text{with} \quad \lambda(1) = 1.$$

For example, since $1728 = 2^6 \cdot 3^3$, we have $\lambda(1728) = (-1)^{6+3} = (-1)^9 = -1$.

(a) Compute $\lambda(30)$ and $\lambda(504)$.

We have $30 = 2 * 3 * 5$ and $504 = 2^3 * 3^2 * 7$, so

$$\lambda(30) = (-1)^{1+1+1} = -1 \quad \text{and} \quad \lambda(504) = (-1)^{3+2+1} = 1.$$

(b) Prove that $\lambda(n)$ is a multiplicative function.

Proof. Write $m = \sum_{p \text{ prime}} p^{k_p}$ and $n = \sum_{p \text{ prime}} p^{j_p}$, where all but finitely many k_p and j_p are 0. Then

$$\lambda(m)\lambda(n) = (-1)^{\sum_p k_p} (-1)^{\sum_p j_p} = (-1)^{\sum_p (k_p + j_p)} = \lambda(mn).$$

(Note there's no requirement that m and n are relatively prime!) □

(c) We now define a new function $G(n)$ by the formula

$$G(n) = \lambda(d_1) + \lambda(d_2) + \cdots + \lambda(d_r),$$

where $1 = d_1 < d_2 < \cdots < d_{r-1} < d_r = n$ are the divisors of n.

Explicitly compute $G(n)$ for each $1 \leq n \leq 18$.

n	$\lambda(n)$	$G(n)$
1	1	1
2	-1	0
3	-1	0
4	1	1
5	-1	0
6	1	0
7	-1	0
8	-1	0
9	1	1
10	1	0
11	-1	0
12	-1	0
13	-1	0
14	1	0
15	1	0
16	1	1
17	-1	0
18	-1	0

It looks like $G(n) = 1$ if n is a perfect square, and 0 otherwise.

(d) Use your computations to make a guess as to the value of $G(n)$. Use your guess to find the value of G(62141689) and G(60119483). (You can find the factorizations of these large numbers on wolframalpha.com.)

It looks like $G(n) = 1$ if n is a perfect square, and 0 otherwise. IF this is the case, then since 62141689 is a perfect square, but 60119483 is not, $G(62141689)$ should be 1, and $G(60119483)$ should be 0.

(e) Prove that your guess in (d) is correct. (Use Exercise 43.)

Proof. Since $\lambda(n)$ is multiplicative, so is $G(n)$. So if $n = \sum_{p \text{ prime}} p^{k_p}$, then

$$G(n) = G\left(\sum_{p \text{ prime}} p^{k_p}\right) = \prod_{p \text{ prime}} G(p^{k_p}).$$

Now,

$$G(p^k) = \sum_{i=0}^{k} \lambda(p^i) = \sum_{i=0}^{k} (-1)^i = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 1 & \text{if } k \text{ is even.} \end{cases}$$

So $G\left(\sum_{p \text{ prime}} p^{k_p}\right)$ is 0 whenever at least one k_p is odd (i.e. when n is note a perfect square) and is 1 otherwise (when n is a perfect square). □

Exercise 45. Let p be an odd prime.

(a) If $a = b^2$ is a perfect square, explain why it is impossible for a to be a primitive root modulo p.

Proof. Since p is odd, the number $(p-1)/2$ is an integer, so we can compute

$$a^{(p-1)/2} = (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

So $|a|_p \leq (p-1)/2 < p-1$, giving that a is not a primitive root modulo p. □

(b) Let g be a primitive root modulo p. Prove that g^k is a quadratic residue modulo p if and only if k is even.

Proof. The list

$$g, g^2, g^3, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$$

gives all of the nonzero numbers modulo p. The even powers are residues, since $g^{2k} = (g^k)^2$. But this is exactly half of the list, so the others are all non-residues. □

(c) If k divides $p-1$, show that the congruence $x^k \equiv 1 \pmod{p}$ has exactly k distinct solutions modulo p.

Proof. We have $x^k \equiv 1 \pmod{p}$ if and only if $|x|_p$ divides k. So the number of solutions is

$$\sum_{d|k} \psi_p(k) = \sum_{d|k} \phi(k) = k.$$

□

Exercise 46. Use the discrete logarithm table for $p = 37$ to find *all* solutions to the following congruences.

(a) $12x \equiv 23 \pmod{37}$

We have $12x \equiv_{37} 23$ if and only if

$$\text{dlog}_2(23) \equiv_{36} \text{dlog}_2(12x) \equiv_{36} \text{dlog}_2(12) + \text{dlog}_2(x).$$

So

$$\text{dlog}_2(x) \equiv_{36} \text{dlog}_2(23) - \text{dlog}_2(12) \equiv_{36} 15 - 28 \equiv_{36} 23.$$

Thus $x \equiv_{37} 2^{23} \equiv_{37} 5$.

(b) $5x^{23} \equiv 18 \pmod{37}$

We have $5x^{23} \equiv_{37} 18$ if and only if

$$\text{dlog}_2(18) \equiv_{36} \text{dlog}_2(5x^{23}) \equiv_{36} \text{dlog}_2(5) + 23\text{dlog}_2(x).$$

So

$$23\text{dlog}_2(x) \equiv_{36} \text{dlog}_2(18) - \text{dlog}_2(5) \equiv_{36} 17 - 23 \equiv_{36} 30.$$

So since $\gcd(23, 36) = 1$, there is one solution. Namely, since

$$23 * 11 + 36 * (-7) = 1,$$

we have

$$\text{dlog}_2(x) \equiv_{36} 30 * 11 = 330 \equiv_{36} 6.$$

So $x \equiv_{37} 2^6 \equiv_{37} 27$.

(c) $x^{12} \equiv 11 \pmod{37}$

We have $x^{12} \equiv_{37} 11$ if and only if

$$\text{dlog}_2(11) \equiv_{36} \text{dlog}_2(x^{12}) \equiv_{36} 12\text{dlog}_2(x).$$

So since $\gcd(12, 36) = 12$, which does not divide $\text{dlog}_2(11) = 30$, there are no solutions.

(d) $7x^{20} \equiv 34 \pmod{37}$

We have $7x^{20} \equiv_{37} 34$ if and only if

$$\text{dlog}_2(34) \equiv_{36} \text{dlog}_2(7x^{20}) \equiv_{36} \text{dlog}_2(7) + 20\text{dlog}_2(x).$$

So

$$20\text{dlog}_2(x) \equiv_{36} \text{dlog}_2(34) - \text{dlog}_2(7) \equiv_{36} 8 - 32 \equiv_{36} 12.$$

Since $\gcd(20, 36) = 4$, which divides 12, there are four solutions. First,

$$20 * 2 + 36 * (-1) = 4,$$

so

$$20 * 2 * 3 \equiv_{36} 4 * 3 = 12.$$

Thus $\text{dlog}_2(x) = 60 \equiv_{36} 24$ is one solution. The others are

$$24 + \frac{36}{4} \equiv_{36} 33, \quad 24 + 2 * \frac{36}{4} \equiv_{36} 6, \quad \text{and} \quad 24 + 3 * \frac{36}{4} \equiv_{36} 15.$$

So

$$x \equiv_{37} 2^{24} \equiv_{37} 10, \quad x \equiv_{37} 2^{33} \equiv_{37} 14, \quad x \equiv_{37} 2^6 \equiv_{37} 27, \quad \text{or } x \equiv_{37} 2^{15} \equiv_{37} 23.$$

Exercise 47. Create a discrete logarithm table for $p = 17$, and use it to find all solutions to $5x^6 \equiv 7 \pmod{17}$.

For the base, you must choose a primitive root. So, in particular, 2 won't work in this example! However, 3 will, so that's what I'm going to use.

The exponential table modulo 17 is

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

,

so the logarithmic table is

b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{dlog}_3(b)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

.

Now, $5x^6 \equiv_{17} 7$ if and only if

$$\text{dlog}_3(7) \equiv_{16} \text{dlog}_3(5x^6) \equiv_{16} \text{dlog}_3(5) + 6\text{dlog}_3(x).$$

So

$$6\text{dlog}_3(x) \equiv_{16} \text{dlog}_3(7) - \text{dlog}_3(5) \equiv_{16} 11 - 5 \equiv_{16} 6.$$

Since $\gcd(6, 16) = 2$, which divides 6, there are two solutions: $\text{dlog}_3(x) \equiv_{16} 1$ or $1 + 16/2 = 9$. So

$$x \equiv_{17} 3^1 = 3, \quad \text{or} \quad x \equiv_{17} 3^9 \equiv_{17} 14.$$