Homework 8, solutions

Solution to 25d). First we find a primitive root modulo 17. It is not hard to see that that 3 is a primitive root modulo 17. Indeed, the order of 3 modulo 17 divides 16. We have $3^2 \equiv -8 = -2^3 (\mod 17)$ so $3^8 \equiv 2^{12} = (2^4)^3 \equiv -1 (\mod 17)$. It follows that order of 3 modulo 17 does not divide 8, hence it must be equal to 16.

Now $3^{16} - 1 = (3-1)(3+1)(3^2+1)(3^4+1)(3^8+1)$ is not divisible by 17^2 so 3 is a primitive root modulo every power of 17 (if $3^{16}-1$ was divisible by 17^2, we would replace 3 by $3+17=20$). Since 3 is odd, it is also a primitive root modulo $2 \cdot 17^m$ (if it was even, we would replace it by $3+16^n$ which would be odd).

Here is a different solution. It is not hard to see that 6 is also a primitive root modulo 17 and 17^2 does not divide $6^{16}-1$. Thus 6 is a primitive root modulo any power of 17. However 6 is even, so to get a primitive root modulo $2 \cdot 17^m$ we use $6+17^m$, which is odd.

Finally, let us remark that if p is an odd prime there is always an odd integer a which is a primitive root modulo p and such that $a^{p-1}-1$ is not divisible by p^2. Such a is a primitive root modulo every power of p and modulo $2p^m$ for every m.

Problem 28a). When $m=2$ the result is obvious. Assume now that $m>2$, so $\phi(m)$ is even. Suppose that a is a primitive root modulo m. Then $a^{\phi(m)/2} \equiv -1 (\mod m)$. Indeed, we have $-1 \equiv a^k (\mod m)$ for some (unique) k such that $0 \leq k < \phi(m)$. But then $a^{2k} \equiv 1 (\mod m)$, so $\phi(m)$ divides $2k$ and therefore $\phi(m)/2$ divides k. The only positive k less than $\phi(m)$ and divisible by $\phi(m)/2$ is $k = \phi(m)/2$. We proved the following:

If a is a primitive root modulo $m>2$ then $\operatorname{ind}_a(-1) = \phi(m)/2$.

Since a is a primitive root modulo m, the numbers $a^0, a^1, \ldots, a^{\phi(m)-1}$ taken modulo m give all the residues modulo m which are relatively prime to m. Thus the product of all the positive integers less than m and relatively prime to m is congruent modulo m to the product

$$a^0 a^1 \ldots a^{\phi(m)-1} = a^{1+2+\ldots+(\phi(m)-1)} = a^{(\phi(m)-1)\phi(m)/2} =$$

$$= (a^{\phi(m)/2})^{\phi(m)-1} \equiv (-1)^{\phi(m)-1} = -1 (\mod m)$$

(in the last step we used the fact that $\phi(m)-1$ is odd.)

Solution to Problem 32c). We know that 3 is a primitive root modulo 17. Thus x is a solution to $8x^{12} \equiv b(\mod 17)$ if and only if

$$\mathrm{ind}_3(8) + 12\mathrm{ind}_3(x) \equiv \mathrm{ind}_3(b)(\mod 16).$$

Now, since $8 \equiv -9(\mod 17)$, we have $\mathrm{ind}_3(8) = \mathrm{ind}_3(-3^2) = \mathrm{ind}_3(-1) + \mathrm{ind}_3(3^2) = 8 + 2 = 10$.

It follows that our original congruence is solvable if and only if the congruence $10 + 12y \equiv \mathrm{ind}_3(b)(\mod 16)$ is solvable, i.e. when $12y \equiv \mathrm{ind}_3(b) - 10(\mod 16)$ is solvable. This happens if and only if $\gcd(12, 16) = 4$ divides $\mathrm{ind}_3(b) - 10$. Among the numbers $0, 1, \ldots, 15$ only $2, 6, 10, 14$ have this property. Thus our congruence is solvable if and only if $\mathrm{ind}_3(b)$ is one of $2, 6, 10, 14$ modulo 16. Note that $3^4 \equiv -4(\mod 17)$. Thus

$$3^6 = 3^2 \cdot 3^4 \equiv 9(-4) = -36 \equiv 15 \equiv -2(\mod 17),$$

$$3^{10} = 3^6 \cdot 3^4 \equiv (-2)(-4) = 8(\mod 17),$$

and

$$3^{14} = 3^{10} \cdot 3^4 \equiv 8(-4) = -32 \equiv 2(\mod 17).$$

Thus our congruence is solvable if and only if b is congruent to one of $2, 8, 915$ modulo 17.

Solution to problem 35. a) Since s, r are primitive roots modulo a prime p, we have $r \equiv s^{\mathrm{ind}_s(r)}(\mod p)$. Thus

$$a \equiv r^{\mathrm{ind}_r(a)} \equiv (s^{\mathrm{ind}_s(r)})^{\mathrm{ind}_r(a)} = s^{\mathrm{ind}_s(r)\mathrm{ind}_r(a)}(\mod p).$$

This means that $\mathrm{ind}_s(a) \equiv \mathrm{ind}_s(r)\mathrm{ind}_r(a)(\mod (p-1))$ (as $\phi(p) = p - 1$).

b) We have proved in the solution to Problem 28a) that if $m > 2$ and a is a primitive root modulo m then $\mathrm{ind}_a(-1) \equiv \phi(m)/2(\mod \phi(m))$. Thus

$$\mathrm{ind}_r(p-a) \equiv \mathrm{ind}_r(-a) \equiv \mathrm{ind}_r(-1) + \mathrm{ind}_r(a) \equiv \frac{p-1}{2} + \mathrm{ind}_r(a)(\mod (p-1)).$$

Solution to Problem 38. Since the set $\{1^n, 2^n, \ldots, (p-1)^n\}$ contains $p-1$ numbers, each relatively prime to p, it suffices to show that no two of these numbers are congruent modulo p. Let r be a primitive root modulo p and $1 \leq a, b < p$. Then $a^n \equiv b^n (\mod p)$ if and only if $\mathrm{ind}_r(a^n) \equiv \mathrm{ind}_r(b^n)(\mod ((p-1))$, i.e. if and only if $n\mathrm{ind}_r(a) \equiv n\mathrm{ind}_r(b)(\mod ((p-1))$. Since n is relatively prime to $p-1$, the last congruence is equivalent to $\mathrm{ind}_r(a) \equiv \mathrm{ind}_r(b)(\mod ((p-1))$ which is the same as $a \equiv b(\mod p)$. This proves that our numbers are indeed all different modulo p and therefore thy form a reduced residue system modulo p.