HW8

Question 3. By theorem 6.2 (i), since ord(a)$|\phi(m)$, ord(a) is no larger than $\phi(m)$. ord(a)=m-1, hence $m-1 \leq \phi(m)$.

$\phi(m)$ is the number of positive integers less than m that are relatively prime to m, hence $\phi(m) \leq m-1$ for all $m > 1$.

Thus $\phi(m) = m-1$. It implies that m is prime (see problem 3.59).

Question 7. ord(x)=4 for prime p. Hence $4|\phi(p) = p-1$. Hence p=4k+1 for all $k \geq 0$.

Question 12. It is clear that $2^{45} = 1 \bmod 2^{45}-1$. But for $1 \leq k < 45$, $2 \leq 2^k < 2^{45}$, so $2^k \neq 1 \bmod 2^{45}-1$.

So the order of 2 is 45 which divides $\phi(2^{45}-1)$. Hence it is a mutliple of 45.

Question 29. There are exactly $\frac{227-1}{2} = 113$ quadratic nonresidues.

Since 227 is prime, by theorem 6.7, there is at least one prime root. Moreover, by theorem 6.13, there are exactly $\phi(\phi(227))$ primitive roots.

$$\phi(\phi(227)) = \phi(226) = \phi(2)\phi(113) = (1)(112) = 112$$

So there are 112 primitive roots.

Note that every primitive root has to be a quadratic nonresidue. (For a quadratic residue, by Euler's criterion, it has order at most $\frac{227-1}{2} = 113$, so all quadratic residues can not be primitve roots).

It means that there is one quadratic nonresidue which is not a primitive root.

Indeed such number is -1. As 227 is 3 mod 4, so -1 is a quadratic nonresidue (by a thoerem in chapter 5). But $(-1)^2 = 1 \bmod 227$, hence it has order 2 and can not be a primitive root.

(b) To generalize this result, look at the above computation of the numbers of quadratic nonresidues and primitive roots. Then you will notice that if $p = 2q+1$, where q is odd prime, will get the desired result.

Proof: $\phi(\phi(p)) = \phi(\phi(2q+1)) = \phi(2q) = \phi(2)\phi(q) = (1)(q-1) = q-1$. So there are q-1 primitive roots. But there are $\frac{2q+1-1}{2} = q$ quadratic nonresidues. And by the same reasoning as above, there is exactly one quadratic nonresidue which is not a primitive root.

Question 34.

(a) By theorem 6.7, every prime has a primitive root so 29 has at least one primitive root. Number of primitive roots is $\phi(\phi(29)) = \phi(28) = \phi(4)\phi(7) = 12$.

Suppose x is a primitive root, then for all $1 \leq k < 29$ such that $(k, 28) = 1$, x^k would account for all primitive roots.

Notice that there is an inverse y such that $xy = 1$ mod 29 (since 29 is prime, such inverse always exists and is unique.). $(xy)^n = (x)^n(y)^n = 1$ mod 29. Hence when $x^n = 1$ mod 29, then we have y^n mod 29. And if $x^n \neq 1$ mod 29, then $y^n \neq 1$ mod 29. It means that order of x and order of y are the same. Hence if x is a primitive root, then y is another primitive root. And in such case, x and y can not equal to each other (because if x=y mod 29 but x and y are inverse to each other, then $xy = 1 = x^2$ mod 29. And x has order at most 2 then it would contradict our assumption that x is a primitive root).

We can pair up such an pair x and its inverse y when we multiply all primitive roots mod 29. Pair up all primtive roots in this way. It implies that the product of all primitive roots is 1 mod 29.

(b) When p=2, then 1 is the only primitve root so the product of primitive roots is 1. When p=3, the only primitive root is 2, so the product of all primitve roots is 2.

But for all other primes, the primitive root must have order greater than 2 (since $\phi(p) = p - 1$ is greater than 2). And we can use exactly the same argument as above. (Note that the above argument in (a) does not use any property of 29 but only the fact that 29 is prime!). Hence, we get that the product of all primitive roots is again 1 mod p.