Exercise help set 6/2011 **Number Theory**

1.

a) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 5 \pmod{7} \\ x \equiv 8 \pmod{15} \end{cases} \iff \begin{cases} x \equiv 2 \equiv 0 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 5 \pmod{7} \\ x \equiv 8 \equiv 3 \pmod{5} \\ (x \equiv 8 \equiv 2 \pmod{3}) \end{cases}$

So $x \equiv 0y + 2z + 5w + 8u \pmod{210}$.

y is not needed.

$z = (210/3) \cdot (210/3)_3^{-1} = 70 \cdot (70)_3^{-1} = 70 \cdot 1_3^{-1} = 70$.

$w = (210/7) \cdot (210/7)_7^{-1} = 30 \cdot (30)_7^{-1} = 30 \cdot 2_7^{-1} = 30 \cdot 4 = 120$.

$u = (210/5) \cdot (210/5)_5^{-1} = 42 \cdot 2_5^{-1} = 42 \cdot 3 = 126$.

$x = 2z + 5w + 8u \equiv 2 \cdot 70 + 5 \cdot 120 + 8 \cdot 126 = 140 + 600 + 1008 = 1748 \equiv \mathbf{68} \pmod{210}$.

b) $\begin{cases} 2x \equiv 3 \pmod{9} \\ 4x \equiv 6 \pmod{10} \\ 6x \equiv 9 \pmod{11} \end{cases} \iff x = \frac{y}{2}$, missä $\begin{cases} y \equiv 0 \pmod{2} \\ y \equiv 3 \pmod{9} \\ 2y \equiv 6 \pmod{10} \\ 3y \equiv 9 \pmod{11} \end{cases}$ eli $\begin{cases} y \equiv 0 \pmod{2} \\ y \equiv 3 \pmod{9} \\ y \equiv 3 \pmod{5} \\ y \equiv 3 \pmod{11} \end{cases}$

So $y = 3z + 3u + 3w \pmod{990}$

$z = (990/9) \cdot (990/9)_9^{-1} = 110 \cdot (110)_9^{-1} = 110 \cdot 2_9^{-1} = 110 \cdot 5 = 550$.

$u = (990/5) \cdot (990/5)_5^{-1} = 198 \cdot (198)_5^{-1} = 198 \cdot 2_5^{-1} = 198 \cdot 2 = 396$.

$w = (990/11) \cdot (990/11)_{11}^{-1} = 90 \cdot (90)_{11}^{-1} = 90 \cdot 2_{11}^{-1} = 90 \cdot 6 = 540$.

$x = \frac{1}{2}(3z+3u+3w) \equiv \frac{1}{2}(3 \cdot 550 + 3 \cdot 396 + 3 \cdot 540) \equiv \frac{3}{2}(550+396+540) \equiv \frac{3}{2} \cdot 1486 \equiv 2229 \equiv 249 \pmod{495}$.

2. *Prove by the Chinese Remainder Theorem: for all $k \in \mathbb{N}$ there exist k consequtive numbers $a+1, \ldots, a+k$ of which all are divisible whith some square (not necessarily the same).*

Apply the Chinese Remainder Theorem to $\begin{cases} x \equiv 1 \pmod{2^2} \\ x \equiv 2 \pmod{3^3} \\ \ldots \\ x \equiv k \pmod{p_k^2} \end{cases}$

3. *Calculate $\varphi(10)$, $\varphi(100)$ and $\varphi(10!)$.*

$$\begin{aligned} \varphi(10) &= \varphi(2)\varphi(5) = (2-1)(5-1) = 4 \\ \varphi(100) &= \varphi(10) = \varphi(2^2)\varphi(5^2) = (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot 20 = 40 \\ \varphi(10!) &= \varphi(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10) = \varphi(2^8 3^4 5^2 7^1) = (2^8 - 2^7)(3^4 - 3^3)(5^2 - 5)(7-1) \\ &= 128 \cdot 54 \cdot 20 \cdot 6 = 829440 \end{aligned}$$

4. *a) For which n is $\varphi(n)$ odd?*

b) For which n is $\varphi(n) = \varphi(2n)$?

a) only n=1 and n=2, since all other contain an odd prime or a higher power of 2 in their canonical decompositions.

b) Exactly all odd. Every even number is on the form $n = 2^\alpha \cdot t$, with t odd, so $\varphi(n) = \varphi(2^\alpha) \cdot \varphi(t) = 2^{\alpha-1}\varphi(t)$ ja $\varphi(2n) = \varphi(2^{\alpha+1}) \cdot \varphi(t) = 2^\alpha \varphi(t)$, whereas for odd $\varphi(2n) = \varphi(2)\varphi(n) = 1 \cdot \varphi(n) = \varphi(n)$.

5. *Find the orders of* 3, 7 *ja* 11 $\pmod{20}$.

4, 4, 2

6. *Find alt least one primitive root modulo* 14.

2 and 5 are primitive roots $\pmod{14}$.

7. 2 *is a primitive root modulo* 101. *Find* $ord_{101}(2^{32})$.

$$(101-1)/(32,(101-1)) = 100/4 = 25.$$

8. 2 *is a primitive root modulo* 19. *How many primitive roots modulo* 19 *exist? After finding out this, find all these primitive roots.*

Since 19 os prime, by thm there are $\varphi(19-1) = \varphi(18) = \varphi(2\cdot 3^2) = \varphi(2)\varphi(3^2) = 6$ primitive roots. By experimenting one finds that they are 2, 3, 10, 13, 14 and 15.

9. *Let* r *be a primitive root modulo* m *and* $(m,a) = 1$. *Prove that the following are equivalent:*

(1) *a is a primitive root modulo* $\pmod{m}$.
(2) *For all prime factors* p *of* $\varphi(m)$*:*

$$a^{\varphi(m)/p} \not\equiv 1 \pmod{m}.$$

(1) $\implies$ (2): If a is a primite root $\pmod{m}$, then $a^j \not\equiv 1 \pmod{m}$ hjolds for all $0 < j < \varphi(m)$.

(2) $\implies$ (1): If a is not a primite root $\pmod{m}$, there exists $k < \varphi(m)$, s. th. $a^k \equiv 1 \pmod{m}$, for example $k = \mathrm{o}rd_m a$. But the order of a subgroups divides the order of the whole group, so $k = \mathrm{o}rd_m a = \# < a > \,|\, \#\mathbb{Z}_m^* = \varphi(m)$ ie. $k \,|\, \varphi(m)$, ie. $\varphi(m) = kp\alpha$ for some prime factor p of $\varphi(m)$ and some number α.

$$1 = a^k = a^{\varphi(m)/(p\alpha)},$$

so

$$a^{\varphi(m)/p} = \left(a^{\varphi(m)/(p\alpha)}\right)^\alpha = 1^\alpha = 1.$$

10. *Construct an index table for* 13. *(Compare with the given table)* .

Take any primite root. I take $r = 2$. (Smallest). calculating all powers $2^n \pmod{13}$ one gets:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind} a$	12	1	4	2	9	5	11	3	8	10	7	6

11. *Which of the following congruences are solvable?*

a) $x^4 \equiv 17 \pmod{67}$
b) $x^4 \equiv 18 \pmod{67}$

c) $x^5 \equiv 17 \pmod{67}$

Solve them using that 2 is a primitive root $\pmod{67}$.

1. method: brute force: list all squares in $\mathbb{Z}_{67}$: One way to calculate avoiding big numbers is to use the fact that $1+3+5+\cdots+(2n+1) = n^2$, so $(n+1)^2 = n^2+(2n+1)$. There are $(67-1)/2 = 33$ squares:

$1, 4, 9, 16, 25, 36, 49, 64, 81 \equiv 4, 33, 54, 77, 102 \equiv 35, 62, 79 \equiv 24, 55, 88 \equiv 21, 56,$

$93 \equiv 26, 65, 106 \equiv 39, 82 \equiv 15, 127 \equiv 60, \equiv 40, 107 \equiv 22, 73 \equiv 6, 126 \equiv 59,$

$114 \equiv 47, 104 \equiv 37, 96 \equiv 29, 90 \equiv 23, 86 \equiv 19,$ ja $84 \equiv \mathbf{17}$.

($67 \equiv 0$ is neither.)

So 17 has a square root: $(\pm 33)^2 \equiv 17 \pmod{67}$. Also 33 has a square root $(\pm 10)^2 \equiv 33 \pmod{67}$, so $10^4 \equiv 17 \pmod{67}$ and $10^4 \equiv 17 \pmod{67}$. Verify by checking that $10000 \equiv 17 \pmod{67}$. (use the pocket calculator: divide 10000-17 by 67 and find that you get 149 , an integer.) On the contrary, $-33 \equiv 34$ has no square root $\pmod{67}$, so ± 10 are the only solutions to $x^4 \equiv 17 \pmod{67}$.

18 is not in the list, so b) is unsolvable. To solve c) by brute force, you need a list of 5:th powers of all numbers (classes) 1...33. ——........

2. method: Find the solution as $a = 2^n$, $1 \le n \le 65 \pmod{66}$. This is OK, since 2 is a primitive root $\pmod{67}$.

$$x^5 \equiv 17(67) \iff 2^{5n} \equiv 17(67) \iff 5n \equiv \operatorname{ind}_2 17(66).$$

I made an index table $\pmod{67}$, wtih prim. root 2 by calculating powrrs of 2 $\pmod{67}$: (not all — too hard)

$n = \mathrm{ind}_2(2^n)$	$2^n \pmod{67}$	
0	$1 \pmod{67}$	
4	$16 \pmod{67}$	
5	$32 \pmod{67}$	
8	$55 \pmod{67}$	
10	$19 \pmod{67}$	
11	$38 \pmod{67}$	
12	$9 \pmod{67}$	
15	$5 \pmod{67}$	
16	$10 \pmod{67}$	
20	$26 \pmod{67}$	
24	$14 \pmod{67}$	
25	$28 \pmod{67}$	
28	$32 \pmod{67}$	
30	$25 \pmod{67}$	
32	$33 \pmod{67}$	
35	$63 \pmod{67}$	
36	$59 \pmod{67}$	
40	$6 \pmod{67}$	
44	$29 \pmod{67}$	
45	$58 \pmod{67}$	
48	$62 \pmod{67}$	
50	$47 \pmod{67}$	
52	$54 \pmod{67}$	
55	$30 \pmod{67}$	
56	$60 \pmod{67}$	
60	$22 \pmod{67}$	
64	$17 \pmod{67}$	
65	$34 \pmod{67}$	
66	$1 \pmod{67}$	(Fermat!)

At last: $\operatorname{ind} 17 = 64 = 4 \cdot 16$, so ex a) is solved by $2^{16} = 10$, like we know already.

b) 1. method: 18 is not in the (complete!) list of squares, so the solution does not exist.

2. method: $\left(\frac{18}{67}\right)$ can be calculated with the reciprocal thm, and becomes -1. No solution!

3. method: Write $n = \operatorname{ind} x$. For $x^4 = 2^{4n} \equiv 18 \pmod{67}$ we must have

$$4n \equiv \operatorname{ind} 18 \pmod{66}$$

same as $\operatorname{ind} 18 = 4n - 66k$ for some $k \in \mathbb{Z}$, which implies that $\operatorname{ind} 18$ is even. Now $\operatorname{ind} 18$ is missing in my list of indices, but 9 is in there, so we calculate $\operatorname{ind} 9 = 12$. So $\operatorname{ind} 18 = \operatorname{ind}(2 \cdot 9) = 1 + 12 = 13$, odd, so there is no solution.

Side remark: $\operatorname{ind}(\pm 3) = \frac{1}{2}(\operatorname{ind} 9 = 6 + k \cdot 66)$ (Really: $2^6 = 64 \equiv -3$, ja $2^3 3 = -1$, so $\operatorname{ind}(3) = 6 + 33 = 29$, which works.)

c) One couls list all 5:th powers of $1 \leq k \leq 66 \pmod{67}$,until one finds the solution, if ever. We use indices instead

$$x^5 \equiv 17(67) \iff 2^{5n} \equiv 17(67) \iff 5n \equiv \operatorname{ind}_2 17(66)$$
$$\iff 5n \equiv 64(66)(\equiv -2(66)).$$

Since $(5, 66) = 1$, we can invert 5 in the ring $\mathbb{Z}_{66}$, so the solution exists. In fact. $5^{-1} = 53 \in \mathbb{Z}_{66}$ can be found with Euclid's algortihm. So

$$n \equiv -2 \cdot 53 \equiv -106 \equiv -40 \equiv 26 \quad (66).$$

and a solution is 2^{26}, by the listit is $2 \cdot 2^{25} \equiv 2 \cdot 28 \equiv 56 \equiv -11$. This does it.