Exercise help set 4/2011 **Number Theory**

1. *a) no square of an integer is of the form* $4n+2$ *or* $4n+3$.
b) the product of 4 consecutive numbers is divisible by 24.
c) the product of k *consecutive numbers is divisible by* $k!$.

a) The sqaure of an even number is $(2m)^2 = 4m^2 = 4n+0$, not $4n+2$ or $4n+3$ (div. algor. uniqueness). The sqaure of an even number is$(2m+1)^2 = 4m^2+4m+1$, not $4n+2$ or $4n+3$ (div. algor. uniqueness).

With congruences: Prove that the congruence $x^2 \equiv 2 \pmod 4$ and $x^2 \equiv 3 \pmod 4$ has no solutions, ie solve the 2 degree equations $x^2 = 2$ and $x^2 = 3$ in the ring $\mathbb{Z}_4$. Easy, because only 4 alternatives. Try all. Since $0^2 = 0$, $1^2 = 1$, $4^2 = 4 = 0$ and $3^2 = 9 = 1$, there are no solutions.

b) Of the 4 numbers 2 are even, one of them divisible by 4. One si div by 3. therefore, the ir product is div by 24.

c) in $\mathbb{N}$, the product of k numbers $a, a+1, \ldots a+k$ is $\frac{(a+k)!}{a!}$. Dividing by $k!$ gives$\frac{(a+k)!}{a!k!} = \binom{a+k}{a} = \binom{a+k}{k} \in \mathbb{N}$, well known to be an ineteger (or see below). For negtive numbers, add to all $mk!$ with large enough m to make them positive. This does not effect calcualtions $\pmod{k!}$.

2. *Take* $x \in \mathbb{R}$, $m \in \mathbb{N}$ *and* $p \in \mathbb{P}$.
a) Prove, that $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$
b) Prove, that $p^{\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \mid m$, *mutta* $p^{1+\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \not| m$.
c) How many zeros are at the end of tjhe decimal expansion of 169! ?
d)Prove directly from the definition that (the binoimial coefficients) $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *are integers*

a) There are no integers in $\left[\frac{\lfloor x \rfloor}{m}, \frac{x}{m}\right[$, since if there were $n \in \left[\frac{\lfloor x \rfloor}{m}, \frac{x}{m}\right[$, we would have $nm \in [\lfloor x \rfloor, x[$,, which is not possible.

b) Denote $k = \prod_{q \in \mathbb{P}} q^{a_q} \in \mathbb{N}$ so the power of p is

$$N_p(k) = N(k) = a_p = \max\{a \in \mathbb{N} \mid p \mid k\}.$$

Try to calcualte $N(m!)$. Of course $N(m!) = N(1 \cdot 2 \cdot 3 \cdot \cdots \cdot m = N(1) \cdot N(2) \cdot N(3) \cdot \cdots \cdot N(m)$, but because p only divides $p, 2p, \ldots$, so

$$\begin{aligned} N(m!) &= N(p) \cdot N(2p) \cdot N(3p) \cdot \cdots \cdot N\left(\left\lfloor \frac{m}{p} \right\rfloor p\right) = N(p \cdot 2p \cdot 3p \cdot \cdots \cdot \left(\left\lfloor \frac{m}{p} \right\rfloor p\right)) \\ &= N(p^{\left\lfloor \frac{m}{p} \right\rfloor} \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \left\lfloor \frac{m}{p} \right\rfloor) = \left\lfloor \frac{m}{p} \right\rfloor + N(1 \cdot 2 \cdot 3 \cdot \cdots \cdot \left\lfloor \frac{m}{p} \right\rfloor) \\ &= \left\lfloor \frac{m}{p} \right\rfloor + N\left(\left\lfloor \frac{m}{p} \right\rfloor\right)! \end{aligned}$$

Repeat this and use a):

$$\begin{aligned} N(m!) &= \left\lfloor \frac{m}{p} \right\rfloor + N\left(\left\lfloor \frac{m}{p} \right\rfloor\right)! = \left\lfloor \frac{m}{p} \right\rfloor + \lfloor \frac{\left\lfloor \frac{m}{p} \right\rfloor}{p} \rfloor + N(\lfloor \frac{\left\lfloor \frac{m}{p} \right\rfloor}{p} \rfloor) \\ &= \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + N(\lfloor \frac{m}{p^2} \rfloor) = \cdots = \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \lfloor \frac{m}{p^3} \rfloor + \ldots \text{äärellinen summa.} \end{aligned}$$

c) Apply b). Since 10 is no prime, we must apply b) to its prime factors. begin with 2 (a bad choice!) :

$$\begin{aligned} N_2(169!) &= \lfloor \tfrac{169}{2} \rfloor + \lfloor \tfrac{169}{2^2} \rfloor + \lfloor \tfrac{169}{2^3} \rfloor + \cdots = \\ &= 84 + 42 + 21 + 10 + 5 + 2 + 1. \end{aligned}$$

Next $p = 5$

$$\begin{aligned} N_5(169!) &= \lfloor \tfrac{169}{5} \rfloor + \lfloor \tfrac{169}{5^2} \rfloor + \lfloor \tfrac{169}{5^3} \rfloor + \cdots = \\ &= 33 + 6 + 1 = 40. \end{aligned}$$

Since the latter (we should have guessed it right out!!) is smaller, 169! is divisible by 10 exactly 40 times.

d) $\binom{n}{k} = \frac{n!}{k!(n-k)! \in \mathbb{N}}$ since it is easy to see by b), that every prime factor of the denominator appears at least equally often in the numerator.

3. ...

a) The multiplication table (mod 11) reveals that tne numbers $1 \ldots 10$ have inverses (mod 11) (in the right order) $1, 6, 4, 3, 9, 2, 8, 7, 5$

b)of the numbers 1–12 only $\varphi(12) = kpl$ are invertible (mod 12) – same a s relative primes to 12, namely 1,5,7 and 11. The multiplication table (mod 12) reveals that tne numbers 1,5,7 and 11 have inverses (mod 12) ovat (in the right order) 1,5,7,11, so all these are inverses of themselves.

It may be easier to consider the representations 1,5,7-12=-5 and 11-12=-1, with inverses 1,5,-5 and -1.

4. ....

$$\begin{aligned} N &= \sum_j a_j 10^j \\ &\equiv a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + \ldots \\ &\equiv a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + a_4 \cdot 3^4 + \ldots \\ &\equiv a_0 + a_1 \cdot 3 + a_2 \cdot 2 + a_3 \cdot (-1) + a_4 \cdot 3 \cdot (-1) + a_5 \cdot 2 \cdot (-1) + \ldots \\ &\equiv (a_0 + a_1 \cdot 3 + a_2 \cdot 2) - (a_3 + a_4 \cdot 3 + a_5 \cdot 2) + \ldots \pmod 7 \end{aligned}$$

$$7 \,|\, n = \prod a_\mu 10^\mu \iff 7 \,|\, (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \ldots$$

5. ...

a) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$

and $\{-1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 20000000000010\}$ are complete (=tjs in Finnish).

$1, 3, 7, 9, 11, 13, 17, 19$ is reduced, so is $-9, -7, -3, -1, 1, 3, 7, 9$. (Yes, these sets have $\varphi(20) = \varphi(5) \cdot \varphi(4) = 4 \cdot 2 = 8$ elements. payb attention ti the symmetry in the latter set.)

b) One complete (tjs) modulo n is $\{1, 2, \ldots, n\}$, so $2 \cdot \sum(tjs.) = n(n+1) \equiv 0$. the smalölest natural number x, satisfying $2x \equiv 0 \pmod n$ is $n/2$, if n iseven and n else.

c) If $n > 2$, then the reduced remainder system (sjs) modulo n can be written $\{-a_1, \ldots, -a_m, a_m, \cdots - a_1\}$, since $(k, n) = (-k, n)$. So $\sum(sjs.) \equiv 0$,and the number is n. If $n = 2$ the sjs is $\{1\}$, with smallest positive representative 1.

6. *a) If* $(m, n) = 1$, *then* x *goes through a t.j.s* $X \pmod m$ *and* y *a t.j.s* $Y \pmod n$,*then the numbers* $xn+my$ *attain all possible values* $\pmod{mn}$. *b) Similarly for reduced systems.*

a) Assume $(m, n) = 1$. We prove that there are nm distinct $\pmod{nm}$ numbers $xn + ym \pmod{nm}$ with $x \in X$, $y \in Y$. .First we prive that they are distinct: If not, then

$$x_1 n + y_1 m \equiv x_2 n + y_2 m \pmod{nm},$$

so, because $(n, m) = 1 \implies n$ is invertible in the ring $\mathbb{Z}_m$,

$$\begin{aligned}
x_1 n + y_1 m &\equiv x_2 n + y_2 m \pmod{nm} \\
(x_1 - x_2)n &\equiv (y_2 - y_1)m \pmod{nm} \\
(x_1 - x_2)n &\equiv (y_2 - y_1)m \equiv 0 \pmod m \quad \Big| \cdot n' \\
(x_1 - x_2) &\equiv 0 \pmod m \\
x_1 &\equiv x_2 \pmod m \\
x_1 &= x_2 \pmod m, \text{ since } x_1, x_2 \in X, \text{ which is a is tjs}
\end{aligned}$$

Similarly $y_1 = y_2$. since trhe congruence classes $xn + ym$ are distinct, there are nm of them.

b) Similar, but one has to prove that $xn+ym$ is in the sjs . $\pmod{mn}$ie invertible in the ring $\mathbb{Z}_{mn}$,when x is invertible $\pmod n$, y is invertible $\pmod m$ and $(m, n) = 1$. We prove that $(xn + ym, nm) = 1$. Since $(n, m) = 1$, we have to prove that $(xn + ym, n) = 1$ and $(xn + ym, m) = 1$. Clearly $(xn + ym, n) = (ym, n) = 1$, since both y and n are relative primes to m . Similarly $(xn + ym, m) = 1$. $\square$. '

7. ....

By Wikipedia: (read more there and in Wolfram's math world)

Just like the Fermat and Solovay–Strassen tests, the Miller–Rabin test relies is an equality or set of equalities that hold true for prime values, then checks whether or not they hold for a number that we want to test for primality.

First, a lemma about square roots of unity in the finite field Z_p, where p is prime and $p > 2$. Certainly 1 and -1 always yield 1 when squared mod p; call these **trivial** square roots of 1.

Lemma: There are no nontrivial square roots of 1 mod p

Proof. This is a a special case of the result that, in a field, a polynomial has no more zeroes than its degree. To show this, suppose that x is a square root of 1 mod p. Then: $x^2 \equiv 1 \pmod p$ ie. $(x - 1)(x + 1) \equiv 0 \pmod p$, which in a field implies $(x + 1) \equiv 0 \pmod p$ or $(x - 1) \equiv 0 \pmod p$. $\square$

Proof proper:Now, let p be an odd prime. Then $p-1$ is even and we can write it as $2^s \cdot d$, where s and d are positive integers, and d is odd. For each $a \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, either

$$a^d \equiv 1 \pmod p$$

or

$$a^{2^r d} \equiv -1 \pmod{p}$$

for some $0 \leq r < s$.

To show that one of these must be true, recall **Fermat's little theorem**: (Choose a such that $p \not| a$.)

$$a^{p-1} \equiv 1 \pmod{p}$$

By the lemma above, if we keep taking square roots of a^{p-1}, we will get either 1 or -1. If we get -1 then the second equality holds and we are done. If we never get -1, then when we have taken out every power of 2, we are left with the first equality. $\square$

Mathematica versions 2.2 and later have implemented the multiple Rabin-Miller test in bases 2 and 3 combined with a Lucas pseudoprime test as the primality test used by the function PrimeQ[n]. As of 1997 no counterexamples are known and if any exist, they are expected to occur with extremely small probability (i.e., much less than the probability of a hardware error is a computer performing the test).

8. *Solve* $x^2 \equiv -1 \pmod{13}$ *using Wilson's thm.*

13 is prime, so by Wilson

$$(13-1)! + 1 \equiv 0 \pmod{13}$$

giving

$$12! \equiv -1 \pmod{13}.$$

Huomataan, että

$$\begin{aligned} 12 &\equiv -1 \pmod{13} \\ 11 &\equiv -2 \pmod{13} \\ 10 &\equiv -3 \pmod{13} \\ &\vdots \\ 7 &\equiv -6 \pmod{13}. \end{aligned}$$

Siis $-1 \equiv 12! \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)^2 \equiv 24^2 \equiv 5^2 \pmod{13}$. Also -5 is a msolution! (others??)