CONCEPTS OF MATHEMATICS, SUMMER 1 2014
ADDITIONAL EXERCISES FOR WEEK 5

(1) If x, y are integers, x divides y and y divides x, then $|x| = |y|$.
(2) In the RSA cryptosystem, explain what could happen if the eavesdropper also has the capability to change the content of the messages Alice and Bob send to each other.
(3) After Alice and Bob managed to exchange public keys, a device is installed on their communication link that allows eavesdroppers to change the content of messages. Alice now would like to send a message to Bob so that Bob is sure that Alice, and not the eavesdroppers, wrote it. Explain how this can be done using the RSA cryptosystem. *Hint: make Alice encrypt a message using her private key.*
(4) (Not really necessary for this course, just if you are interested) Alice and Bob physically meet in a private place and exchange a sequence of randomly generated numbers k_0, k_1, ..., k_n (for n very big, and each k_i much bigger than any possible message they could send to each other). Explain why Alice and Bob are now able to communicate securely without RSA (whose security is unproven).
(5) Fix distinct primes p_1, p_2, ..., p_n. How many different numbers can be obtained by multiplying at most k of those primes together (repetitions are allowed). For example, if $k = n = 2$, $p_1 = 2$, $p_2 = 3$, then we can build 5 numbers: 1 (the empty product), 2, 3, $4 = 2 \cdot 2$, and $6 = 2 \cdot 3$.
(6) Assume m, n, and k are integers. Show that if m and n are coprime and both divide k, then mn divide k.
(7) The *least common multiple* of m and n (written $\operatorname{lcm}(m, n)$) is the minimal natural number divisible by both n and m. For example, $\operatorname{lcm}(15, 20) = 60$. Show that $\operatorname{lcm}(m, n) \cdot \gcd(m, n) = m \cdot n$.
(8) Assume $a^2 + b^2 = c^2$ for integers a, b, c.
    (a) Could it be that a and b are both odd? Why or why not?
    (b) Show that if c is divisible by 3, then both a and b are also divisible by 3.
(9) Train your computational skills. Make up an example to compute: inverse / primality / chinese remainder theorem / Bézout's lemma, gcd, etc.
(10) Fix a prime p. For x an integer such that $x \not\equiv 0 \bmod p$, the *order* of x modulo p is the minimum positive natural number k such that $x^k \equiv 1 \bmod n$.
    (a) Show that every element has an order (i.e. such a k always exists).
    (b) Show that if k is the order of x, then k divides $p - 1$.
    (c) Show that if k is the order of x and l is the order of y, then the order of xy is at most $\operatorname{lcm}(k, l)$. Give an example where they are equal and an example where the order is strictly less. Show that if k and l are coprime, then the order of xy is kl.

Date: June 19, 2014.

(d) Show that if k is the order of x and n divides k, then the order of x^n is $\frac{k}{n}$.

(11) Assume n, x and y are integers. Prove or disprove the following statements. Also say how their truth value changes if we assume in addition that n is prime.
   (a) If $xy \equiv 0 \bmod n$, then $x \equiv 0 \bmod n$ or $y \equiv 0 \bmod n$.
   (b) If $x \not\equiv 0 \bmod n$, then x has an inverse modulo n.
   (c) If x and y have an inverse modulo n, then xy has an inverse modulo n.
   (d) If x and y have an inverse modulo n and x and y are coprime, then $x+y$ has an inverse modulo n.

(12) Give a proof of the Chinese remainder theorem using induction on the number of equations.

(13) Fix an $n \geq 2$. Show that we *cannot* define a relation $x < y \bmod n$ satisfying:
   (a) Antisymmetry: for any $x \equiv y \bmod n$, it is false that $x < y \bmod n$.
   (b) Transitivity: if $x < y < z \bmod n$, then $x < z \bmod n$.
   (c) If $x < y \bmod n$, then $x + z < y + z \bmod n$.

(14) (Hard) The US Government goes mad again: it decides to issue m-dollar bills and n-dollar bills for $0 < m < n$ coprime natural numbers and declares that everything has to be paid using these bills. Show that all amounts strictly above $mn - m - n$ can be paid using only these bills. *Hint: The amounts* 0*,* m*,* $2m$*,* $3m$*, ...,* $(n-1)m$ *can be paid. Argue they are distinct modulo* n *and use this to conclude.*

(15) Three pirates find a treasure buried on an island. After digging it out, they are tired and decide they will split it equally between themselves the next day. The pirates are suspicious of one another, so during the night, the first pirate decides to go take her share: she wakes up, makes three equal piles of coins, throws away the one remaining coin in the ocean, and takes the content of one pile. The second pirate wakes up, and does the same: again, one remaining coin is thrown in the ocean. The third pirate does the same and throws two remaining coins in the ocean. The next day, they evenly split what is left (no coin is left over). What is the smallest possible amount of coins the treasure could have contained?

(16) n fully rational prisoners are walking in line. Each is wearing a hat that has a number from 0 to $m-1$ (it could be that n is much bigger than m). A prisonner cannot see the number on her/his hat, but can see the number on the hats of the prisoners in front of her/him. The jailers inform the prisoners that they will ask each of them in turn for the number on their hats, starting with the prisoner that is last in line (who can see all the other hats). If a prisoner does not reply correctly or tries to communicate she/he is instantly shot. The other prisoners can still hear what happens. The last prisoner in line decides to save the day and manages to shout one number (from 0 to $m-1$) before getting shot. Explain what a smart choice for that number would be and how the other prisoners can then save themselves. *Hint: first solve this problem for* $m = 2$*.*

(17) (Hard) show that if a positive natural number n is the product of k consecutive natural numbers, then n is divisible by $k!$.

(18) Show that there are infinitely many primes congruent to -1 modulo 4.
(19) (Very hard) Show that if m and n are coprime, then $m^{\varphi(n)} \equiv 1 \bmod n$. Explain how this generalizes Fermat's little theorem.
(20) Use modular arithmetic to show that $k-1$ divides $k^n - 1$ (for n a natural number and k an integer). Give another proof that does not use modular arithmetic.
(21) Show that for any integer n, $n^3 + 5n$ is divisible by 6.
(22) (A bit tedious) Show that at least one day of the year (even in leap years) must be a Friday the 13th.