CS:1010 DISCRETE STRUCTURES

PRACTICE QUESTIONS
LECTURE 8

Instructions

- Try these questions before class. Do not submit!

(1) Prove or disprove that if $a \mid bc$, where a, b, and c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.

Not true since $12 \mid 3 \cdot 4$ but 12 does not divide 3 or 4. Similarly, $8 \mid 24$ but 8 does not divide 6 or 4.
But what happens if we consider a to be a prime? Then it is true by Euclid's Lemma.

(2) What are the quotient and remainder when: a) -1 is divided by 3 and b) 3 is divided by 5.

a) $-1 = 3 \cdot (-1) + 2$, so $q = -1$ and $r = 2$.
b) $3 = 0 \cdot 5 + 3$, $q = 0, r = 3$.

(3) What time does a 12-hour clock read
a) 80 hours after it reads $11:00$ and
b) 40 hours before it reads $12:00$?

Since it is a 12 hour clock so we do modulo 12:
a) $11 + 80$ mod $12 = 7$, the clock reads $7:00$.
b) $12 - 40$ mod $12{=}{-28}$ mod $12 = -28 + 36$ mod $12 = 8$, the clock reads $8:00$.

(4) Suppose that a and b are integers, $a \equiv 4(mod 13)$, and $b \equiv 9(mod 13)$.Find the integer c with $0 \leq c \leq 12$ such that
a)$c \equiv a + b(mod\ 13)$
b) $c \equiv a^3 - b^3(mod\ 13)$.

This is a simple exercise of computing the expression, dividing by 13 and taking the nonnegative remainder.
a) $4 + 9$ mod $13 = 13$ mod $13 = 0$. and b) $4^3 - 9^3 = -665$ mod $13 = 11$ since $-665 = -52 \cdot 13 + 11$.

(5) Show that if a, b, c, and m are integers such that $m \geq 2$,$c > 0$, and $a \equiv b(mod\ m)$, then $ac \equiv bc(mod\ mc)$.

Since $a \equiv b(mod\ m)$, there is an integer k s.t. $a - b = km$. Thus $ac - bc = k(mc)$ and $ac \equiv bc(mod\ mc)$.

(6) Show using mathematical induction that if a, b and m are integers such that $m \geq 2$,and $a \equiv b(\text{mod } m)$,then $a^n \equiv b^n \pmod{m}$ for all $n \in \mathbb{N}$.

Basis Step: Since $a^0 = b^0 = 1$ we have $a^0 \equiv b^0 \bmod m$.
Inductive Step: Let $k \in \mathbb{N}$ and assume that $a^k \equiv b^k \bmod m$. We have $a \equiv b(\text{mod } m)$.
We have the theorem : If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$. Using that result we have $a^k \cdot a \equiv b^k \cdot b \bmod m$ and thus $a^{k+1} \equiv b^{k+1} \bmod m$.
With the basis step and inductive step done by the principle of M.I. we have that the result is true for all n.

(7) Convert $(ABCDEF)_{16}$ from hexadecimal to its binary expansion.

We write binary equivalent of each digit and obtain the expansion: 1010 1011 1100 1101 1110 1111.

Expand $B7B$ then again do the same thing: 1011 0111 1011.

(8) Show that the hexadecimal expansion of a positive integer can be obtained from its binary expansion by grouping together blocks of four binary digits, adding initial zeros if necessary, and translating each block of four binary digits into a single hexadecimal digit.

We will have to add upto three 0s in the beginning. Let such a binary representation be: $(\ldots b_{23}b_{22}b_{21}b_{20}b_{13}b_{12}b_{11}b_{10}b_{03}b_{02}b_{01}b_{00})_2$.
The value is $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + 16b_{10} + 32b_{11} + 64b_{12} + 128b_{13} + 16^2 b_{20} + 16^2 \cdot 2b_{21} + 16^2 \cdot 4b_{22} + 16^2 \cdot 8b_{23} + \cdots$ which we rewrite as

$$b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + (b_{10} + 2b_{11} + 4b_{12} + 8b_{13})2^4 + (b_{20} + 2b_{21} + 4b_{22} + 8b_{23})2^8 + \cdots$$

In our grouping, $(b_{i3}b_{i2}b_{i1}b_{i0})_2$ is one hexadecimal digit h_i. Therefore our number is

$$h_0 + h_1 \cdot 2^4 + h_2 \cdot 2^8 + \cdots = h_0 + h_1 \cdot 16 + h_2 \cdot 16^2 + \cdots$$

the hexadecimal expansion.

(9) Prove that for every positive integer n, there are n consecutive composite integers.

Consider the numbers,

$$2 + (n+1)!, 3 + (n+1)!, \dots, n + (n+1)!, (n+1) + (n+1)!$$

There are n such numbers, to show that they are composite.

If $k \leq m$, then $k \mid m!$. Thus for all $2 \leq k \leq (n+1)$, we have that $k \mid (n+1)!$. Also $k \mid k$. Also note if $k \mid a$ and $k \mid b$ then $k \mid (a+b)$. Thus,

$$\begin{aligned} 2 &\mid 2 + (n+1)! \\ 3 &\mid 3 + (n+1)! \\ &\vdots \\ n &\mid n + (n+1)! \\ n+1 &\mid n+1 + (n+1)! \end{aligned}$$

so all of these numbers, having proper divisors, must be composite. Note that these numbers might not have any divisors in common.

(10) Show that if $a^m + 1$ is composite if a and m are integers greater than 1 and m is odd.

From factoring result we have $a + 1$ is a factor of $a^m + 1$. This is true only for odd m. Why?
We have $1 < a + 1 < a^m + 1$ since a and m are greater than 1. Thus we have $a^m + 1$ has a proper factor and is composite.

(11) Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer n.

Suppose m has an odd factor $l > 1$. With $k = m/l$ and l being odd we write,

$$a^m + 1 = (a^k)^l + 1 = (a^k + 1)(a^{k(l-1)} - a^{k(l-2)} + \cdots + -a^k + 1)$$

As we saw above such a factoring is possible only because we assumed l is odd. Since $l > 1$, $k < m$ and $2^k + 1$ is strictly less than $2^m + 1$. This implies $(a^{k(l-1)} - a^{k(l-2)} + \cdots + -a^k + 1) > 1$. Also since $a \neq 0$ implies $(a^k + 1) > 1$. So we have factored $a^m + 1$ into two factors and therefore cannot be prime.

(12) Find the last digit of 7^{100}.

$$7^{100} \equiv (7^2)^{50} \equiv 49^{50} \equiv (-1)^{50} \equiv 1 \bmod 10.$$

(13) In year N, the 300th day of the year is a Tuesday. In year $N+1$, the 200th day is also a Tuesday. On what day of the week did the 100th day of the year $N-1$ occur?

There are either $65+200=265$ or $66+200=266$ days between the first two dates depending upon whether or not year N is a leap year. Since 7 divides into 266, then it is possible for both dates to be Tuesday; hence year N is a leap year and $N-1$ is not a leap year. There are $265+300=565$ days between the date in years N, $N-1$, which leaves a remainder of 5 upon division by 7. Since we are subtracting days, we count 5 days before Tuesday, which gives us Thursday.

(14) P.T. $2^n + 6 \cdot 9^n$ is always divisible by 7 for any positive integer n.

$$2 \equiv 9 \bmod 7 \Rightarrow 2^n \equiv 9^n \bmod 7 \Rightarrow 2^n + 6 \cdot 9^n \equiv 7 \cdot 9^n \equiv 0 \bmod 7.$$