MATH 42
MIDTERM 2
20 MARCH 2015

Name : Solutions

- The time limit is 50 minutes.
- No calculators or notes are permitted.
- Each problem is worth 5 points.

1	/5	**2**	/5
3	/5	**4**	/5
5	/5	**6**	/5
		$\sum$	/30

(1) When the students in a classroom divide into groups of nine, there are four students left over. When the students break into groups of eleven, there is one student left over. Assuming that there are fewer than 100 students in the room, how many students must there be?

$n \equiv 4 \bmod 9$

$n \equiv 1 \bmod 11$ $\quad 0 \leq n \leq 99$

$n = 4 + 9k$, where

$4 + 9k \equiv 1 \bmod 11$

$\Leftrightarrow 9k \equiv -3 \bmod 11.$

Need an inverse of 9 modulo 11:

(11)

(9)

$[2] = (11) - (9)$

$[1] = (9) - 4[2] = (9) - 4(11) + 4(9)$

$= 5(9) - 4(11)$

$\Rightarrow 5 \cdot 9 \equiv 1 \bmod 11.$

Thus

$9k \equiv -3 \bmod 11$

$\Leftrightarrow \underbrace{5 \cdot 9}_{\equiv 1} k \equiv -5 \cdot 3 \bmod 11$

$\Leftrightarrow k \equiv -15 \equiv 7 \bmod 11.$

So

$n = 4 + 9 \cdot (7 + 11 \cdot h) = 4 + 63 + 99h$

i.e. $n \equiv 67 \bmod 99.$

There are $\boxed{\text{67 students,}}$ since $n < 100.$

(2) What is the remainder when 10^{100} is divided by 19?

gcd(10,19) = 1 & 19 is prime, so by Fermat's little theorem:

$$10^{100} = 10^{90} \cdot 10^{10} = (10^{18})^5 \cdot 10^{10}$$
$$\equiv 10^{10} \bmod 19.$$

Method 1

$10^1 \equiv 10$
$10^2 \equiv 100 \equiv 5$
$10^4 \equiv 5^2 \equiv 25 \equiv 6$
$10^8 \equiv 6^2 \equiv 36 \equiv -2$
$\Rightarrow 10^{10} \equiv 10^8 \cdot 10^2$
$\equiv -2 \cdot 5 \equiv -10$
$\equiv 9 \bmod 19$

Method 2

Compute 10 to these exponents (in reverse order):
10, 5, 4, 2, 1.

$10^1 \equiv 10$
$10^2 \equiv 100 \equiv 5$
$10^4 \equiv 25 \equiv 6$
$10^5 \equiv 6 \cdot 10 \equiv 60 \equiv 3$
$10^{10} \equiv 3^2 \equiv 9 \bmod 19$

Method 3

Just mult. by 10 ten times:

$10^1 \equiv 10$
$10^2 \equiv 100 \equiv 5$
$10^3 \equiv 50 \equiv 12$
$10^4 \equiv 120 \equiv 6$
$10^5 \equiv 60 \equiv 3$
$10^6 \equiv 30 \equiv 11$
$10^7 \equiv 110 \equiv 15$
$10^8 \equiv 150 \equiv 17$
$10^9 \equiv 170 \equiv 18$
$10^{10} \equiv 180 \equiv 9.$

Using any method, $10^{100} \equiv 10^{10} \equiv 9 \bmod 19$.

So the remainder is $\boxed{9}$.

(3) (a) How many numbers between 1 and 1500 inclusive are relatively prime to 1500 (that is, share no common factors besides 1 with 1500)?

(b) Find the remainder when 1493^{2002} is divided by 1500.

a) $\varphi(1500) = \varphi(3\cdot 5\cdot 2^2\cdot 5^2) = \varphi(2^2\cdot 3\cdot 5^3)$

$= (4-2)(3-1)(125-25)$

$= \boxed{400}$.

b) Euler's thm:

$2002 \equiv 2 \bmod \varphi(1500)$ and $\gcd(1493, 1500)$

$= \gcd(1500, 7) = 1$

$\Rightarrow 1493^{2002} \equiv 1493^2 \bmod 1500.$

Now observe $1493 \equiv (-7) \bmod 1500$

so $1493^2 \equiv (-7)^2 \equiv 49 \bmod 1500.$

The remainder is $\boxed{49.}$

(4) Suppose that Bob's RSA public key is $(33, 13)$. Alice sends Bob the cipher text $c = 8$. What was Alice's plain text?
(Recall that if s is Alice's plain text, then she computes the cipher text c by computing the remainder when s^{13} is divided by 33.)

$\varphi(33) = \varphi(3\cdot 11) = (3-1)\cdot(11-1) = 20.$

Deciphering exponent: inverse of 13 mod 20.

(20)
(13)
$[7] = (20)-(13)$
$[6] = (13)-[7] = 2\cdot(13)-(20)$
$[1] = [7]-[6] = 2\cdot(20)-3\cdot(13).$

So the inverse is -3, or $\underline{17 \bmod 20}$.

Therefore

$s \equiv c^{17} \bmod 33$
$\equiv 8^{17}.$

Succ. squaring:
$8^1 \equiv 8$
$8^2 \equiv 64 \equiv -2$
$8^4 \equiv (-2)^2 \equiv 4$
$8^8 \equiv 16$
$8^{16} \equiv 256 \equiv 58 \equiv -8$
$8^{17} \equiv 8^{16}\cdot 8 \equiv (-8)8 \equiv -64 \equiv \underline{2 \bmod 33}$

So the secret is $\boxed{2}$.

Alt. solution (w/CRT):

Solve separately:
$s^{13} \equiv 8 \bmod 3$
$\Leftrightarrow s \equiv 8 \bmod 3$ (Fermat)
$\Leftrightarrow \underline{s \equiv 2 \bmod 3}$
and $s^{13} \equiv 8 \bmod 11$
$\Leftrightarrow s^3 \equiv 8 \bmod 11$ (Fermat)
$\Leftrightarrow s \equiv 8^7 \bmod 11$
(since $7\cdot 3 \equiv 1 \bmod \varphi(11)$)

succ. sq. mod 11:
$8^1 \equiv 8$
$8^2 \equiv 64 \equiv 9$
$8^3 \equiv 72 \equiv 6$
$8^6 \equiv 36 \equiv 3$
$8^7 \equiv 3\cdot 8 \equiv 2$

so $s \equiv 2 \bmod 11$.

now, since
$s \equiv 2 \bmod 3$
& $s \equiv 2 \bmod 11$
it follows by CRT that
$s \equiv 2 \bmod 33.$

(5) (a) Let p be an *odd* prime (i.e. a prime besides 2), and k be a positive integer. Prove that if $a^2 \equiv 1 \pmod{p^k}$, then either $a \equiv 1 \pmod{p^k}$ or $a \equiv -1 \pmod{p^k}$.

(b) Find all integers a between 1 and 63 inclusive such that $a^2 \equiv 1 \pmod{64}$.

a) $a^2 \equiv 1 \bmod p^k \iff (a+1)(a-1) \equiv 0 \bmod p^k$

$\iff p^k \mid (a+1)(a-1)$.

Now, since $a+1$ & $a-1$ differ by 2, and $\underline{p>2}$, p can divide at most one of $(a+1)(a-1)$, and p^k is relatively prime to the other (since the only possible common prime factor is p).

Therefore, whichever of $a+1, a-1$ is divis. by p is in fact divis. by p^k. Hence

either $p^k \mid (a+1)$ or $p^k \mid (a-1)$

i.e. either $a \equiv -1 \bmod p^k$ or $a \equiv 1 \bmod p^k$,

as desired.

b) $64 = 2^6$, and $p=2$ so <u>part (a) doesn't apply</u>. Like in (a), we must have $64 \mid (a+1)(a-1)$, but now <u>both</u> $a+1$ & $a-1$ will be even. At most one is divis. by 4, however, so for 64 to divide $(a+1)(a-1)$, it is necessary (and sufficient) for 32 to divide one of $a+1, a-1$ (since 2 will automatically divide the other).

Therefore $a^2 \equiv 1 \bmod 64 \iff a \equiv \pm 1 \bmod 32$.

The possible a in $\{1, 2, \cdots, 63\}$ are $\boxed{1, 31, 33, \text{and } 63.}$

(6) Let $d(n)$ denote the number of divisors of n, including 1 and n. For example:

$$\begin{aligned} d(10) &= 4 \text{ (the divisors are } 1, 2, 5, 10) \\ d(17) &= 2 \text{ (the divisors are } 1, 17) \\ d(24) &= 8 \text{ (the divisors are } 1, 2, 3, 4, 6, 8, 12, 24) \end{aligned}$$

You may assume the following fact: if $\gcd(m, n) = 1$, then $d(mn) = d(m)d(n)$ (I encourage you to try to prove it, but you don't need to do it now).

(a) Find a formula for $d(p^k)$, where p is prime and $k \geq 1$.
(b) Compute $d(91000)$.
(c) Give a simple criterion to tell whether $d(n)$ is even or odd.

a) The divisors are $1, p, p^2, \cdots, p^k$; there are k of them.

$$\boxed{d(p^k) = k+1}$$

b) $91000 = 91 \cdot 10^3 = 7 \cdot 13 \cdot 2^3 \cdot 5^3$

so $d(91000) = d(7)d(13)\,d(2^3)\,d(5^3)$

$= \cancel{4}2 \cdot 2 \cdot 4 \cdot 4$

$= \boxed{64}$

c) If $n = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$ ($p_1, \cdots, p_\ell$ distinct primes)

then $d(n) = (e_1+1)(e_2+1) \cdots (e_\ell+1)$.

Hence $d(n)$ is odd $\iff$ every exponent e_i is even

$\iff$ n is a perfect square.

Squares have an odd number of divisors,
non-squares have an even number of divisors.

Alt. solution: any divisor d has a "partner" n/d. The only divisor that is its own partner is $\sqrt{n}$ (if it's an integer).
So if n isn't a square $d(n)$ is even (divisors are paired up in couples) but if n is a square then $\sqrt{n}$ is left over after this pairing-off.

(additional space for work)