

MATH 42
FINAL EXAM
11 MAY 2015

Name : Solutions

- The time limit is 3 hours.
- No calculators or notes are permitted.
- The last page is a multiplication table for arithmetic modulo 29, which will be useful for several problems. You may detach it from the packet for ease of use if you wish.

1	/20	2	/5	3	/5
4	/5	5	/5	6	/5
7	/5	8	/5	9	/5
10	/6	11	/7	12	/7
Σ					/80

- (1) **Short answer questions.** Each answer is worth 2 points. You do not need to show any work. **Several questions have multiple possible answers; you only need to give one.**

- (a) Compute the greatest common divisor of 77 and 91.

$$\begin{aligned} 91 - 77 &= 14 \\ 77 - 5 \cdot 14 &= \textcircled{7} \\ 14 - 2 \cdot 7 &= 0 \end{aligned}$$

Answer: 7

- (b) Find a perfect number (that is, a positive number which is equal to the sum of all of its divisors, including 1 and itself).

Answer: 6 (also 28, 496, etc.)

- (c) Find an integer x such that $3x \equiv 4 \pmod{7}$.

$$3 \cdot 6 = 18 = 4$$

Answer: 6 (or 13, 20, 27, etc.)

- (d) Find the smallest *positive* number of the form $15x + 39y$, where x and y are integers (positive or negative).

$$\begin{aligned} \gcd(15, 39) \\ &= \gcd(15, 9) \\ &= \gcd(6, 9) \\ &= \gcd(6, 3) = 3 \end{aligned}$$

Answer: 3

- (e) Find a positive integer n such that $10^n \equiv 1 \pmod{113}$. (The number 113 is prime)

Answer: 112 (F.L.T.)

(f) Evaluate $\phi(130)$.

$$130 = 2 \cdot 5 \cdot 13$$
$$\phi(130) = 1 \cdot 4 \cdot 12$$

Answer: 48

(g) Find an integer x , between 0 and 28 inclusive, such that $x^2 \equiv -1 \pmod{29}$. (You may wish to use the multiplication table on the last page.)

Answer: 12 or 17 (only one needed)

(h) Evaluate the Legendre symbol $\left(\frac{-2}{37}\right)$.

$$\left(\frac{-1}{37}\right) \cdot \left(\frac{2}{37}\right)$$

$$= 1 \cdot (-1)$$

(since $37 \equiv 1 \pmod{4}$ & $37 \equiv 5 \pmod{8}$)

Answer: -1

(i) Find a primitive root of 7.

power of 2: 2 4 1 ...
of 3: 3 2 6 4 5 1 ...
of 4: 4 2 1 ...
of 5: 5 4 6 2 3 1 ...
of 6: 6 1 ...

Answer: 3 or 5 (only one needed)

(j) Find a number n , greater than 100, which is *not* a sum of two squares (the number 0 is considered a square).

Answer: 102 (many other possible answers)

(20 points)

(2) Solve the following congruence.

$$123x \equiv 3 \pmod{301}$$

Your answer should be in the form $x \equiv a \pmod{m}$, where a is between 0 and $m - 1$ inclusive.

Extended Euclidean algorithm:

$$\begin{aligned} & (301) \\ & (123) \\ [55] &= (301) - 2(123) \\ [13] &= (123) - 2[55] \\ &= 5(123) - 2(301) \\ [3] &= [55] - 4[13] \\ &= 9(301) - 22(123) \\ [1] &= [13] - 4[3] \\ &= 5(123) - 2(301) - 36(301) + 88(123) \\ &= 93(123) - 38(301) \end{aligned}$$

So 93 is the inverse of 123 modulo 301.

$$93 \cdot 123x \equiv 93 \cdot 3 \pmod{301}$$

$$\boxed{x \equiv 279 \pmod{301}}$$

(5 points)

(3) Solve the following pair of congruences.

$$x \equiv 3 \pmod{15}$$

$$x \equiv 13 \pmod{16}$$

Your answer should be a *single* congruence of the form $x \equiv a \pmod{m}$, where a is between 0 and $m - 1$ inclusive.

$$x = 3 + 15k \quad (\text{for some } k \in \mathbb{Z})$$

$$3 + 15k \equiv 13 \pmod{16}$$

$$15k \equiv 10 \pmod{16}$$

$$-k \equiv 10 \pmod{16}$$

$$k \equiv -10 \pmod{16}$$

$$\equiv 6 \pmod{16}$$

$$\Rightarrow k = 6 + 16h \quad (\text{for some } h \in \mathbb{Z})$$

$$\begin{aligned} \Rightarrow x &= 3 + 15(6 + 16h) \\ &= 3 + 90 + 240h \\ &= 93 + 240h \end{aligned}$$

$$\boxed{x \equiv 93 \pmod{240}}$$

Alt. solution:

$$x = 13 + 16k$$

$$\Rightarrow 13 + 16k \equiv 3 \pmod{15}$$

$$16k \equiv -10 \pmod{15}$$

$$1 \cdot k \equiv 5 \pmod{15}$$

$$\Rightarrow x = 13 + 16(5 + 15h)$$

$$= 13 + 80 + 240h$$

$$\text{ie. } x \equiv 93 \pmod{240}.$$

(5 points)

(4) For each of the following four numbers (with factorization into primes given), either write the number as a sum of two squares or state that it is impossible to do so.

(a) $962 = 2 \cdot 13 \cdot 37$

$$\begin{aligned} 2 &= 1^2 + 1^2 \\ 13 &= 3^2 + 2^2 \\ \Rightarrow 2 \cdot 13 &= (1 \cdot 3 + 1 \cdot 2)^2 + (1 \cdot 2 - 1 \cdot 3)^2 \\ &= 5^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 37 &= 6^2 + 1^2 \\ \Rightarrow 2 \cdot 13 \cdot 37 &= (5 \cdot 6 + 1 \cdot 1)^2 + (5 \cdot 1 - 1 \cdot 6)^2 \\ &= \boxed{31^2 + 1^2} \end{aligned}$$

other poss. answer: $\boxed{29^2 + 11^2}$

(b) $1189 = 29 \cdot 41$

$$\begin{aligned} 29 &= 5^2 + 2^2 \\ 41 &= 5^2 + 4^2 \end{aligned}$$

$$\begin{aligned} \Rightarrow 29 \cdot 41 &= (5 \cdot 5 + 2 \cdot 4)^2 + (5 \cdot 4 - 2 \cdot 5)^2 \\ &= \boxed{33^2 + 10^2} \quad \text{other poss. ans. } \boxed{17^2 + 30^2} \end{aligned}$$

(c) $1725 = 3 \cdot 5^2 \cdot 23$

3 & 23 are primes $\equiv 3 \pmod{4}$ occurring an odd number of times in the prime factorization

$$\Rightarrow \boxed{\text{impossible}}$$

(d) $6137 = 17 \cdot 19^2$

$$17 = 4^2 + 1^2$$

$$\begin{aligned} \Rightarrow 17 \cdot 19^2 &= (4 \cdot 19)^2 + (1 \cdot 19)^2 \\ &= \boxed{76^2 + 19^2} \end{aligned}$$

(5 points)

(5) Prove that $\sqrt{7}$ is irrational.

↪ Suppose for the sake of contradiction that $\sqrt{7} \in \mathbb{Q}$.
Then $\sqrt{7} = a/b$, where a, b are relatively prime
positive integers ($\sqrt{7}$ is a reduced fraction).

Therefore $a^2 = 7b^2$

So $7|a^2$, hence $7|a$ (since 7 is prime).
Therefore in fact $7^2|a^2$, so

$$\begin{aligned} 7^2 &| 7b^2 \\ \Rightarrow 7 &| b^2 \\ \Rightarrow 7 &| b \quad (\text{since 7 is prime}). \end{aligned}$$

Therefore a, b have 7 as a common factor,
which is a contradiction. ↪

The hypothesis must have been false; therefore

$$\underline{\sqrt{7} \notin \mathbb{Q}}.$$

Alt. solution:

Note that a, b must both be odd, because if either one is even then $a^2 = 7b^2$ implies the other is also even; since $\gcd(a, b) = 1$ this is impossible.
Now, all odd squares are $\equiv 1 \pmod{4}$, so $a^2 = 7b^2$ implies $1 \equiv 7 \pmod{4}$, which is a contradiction.

(5 points)

- (6) (a) List all of the prime numbers between 70 and 100.

71, 73, 79, 83, 89, 97.

- (b) For which of these prime numbers p does $x^2 \equiv 5 \pmod{p}$ have an integer solution x ?

$$x^2 \equiv 5 \pmod{p} \text{ has a solution } \Leftrightarrow \left(\frac{5}{p}\right) = 1$$

$$\Leftrightarrow \left(\frac{p}{5}\right) = 1 \quad (\text{quad. reciprocity, using } 5 \equiv 1 \pmod{4})$$

$$\Leftrightarrow p \equiv 1 \text{ or } 4 \pmod{5} \text{ (these are the quad. residues mod 5).}$$

So $x^2 \equiv 5 \pmod{p}$ has a solution for $p = 71, 79, 89$ but not the others.

- (c) For which of these prime numbers p does $x^2 \equiv 3 \pmod{p}$ have an integer solution x ?

By quadratic reciprocity, $\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod{4} \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod{4} \end{cases}$ (since $3 \equiv 3 \pmod{4}$)

So:

$$\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

$$\left(\frac{3}{73}\right) = +\left(\frac{73}{3}\right) = +\left(\frac{1}{3}\right) = 1$$

$$\left(\frac{3}{79}\right) = -\left(\frac{79}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

$$\left(\frac{3}{83}\right) = -\left(\frac{83}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

$$\left(\frac{3}{89}\right) = \left(\frac{89}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$x^2 \equiv 3 \pmod{p}$ has a solution

for $p = 71, 73, 83, 97$

but not the other two.

(5 points)

- (7) You are trying to read a certain 5-digit number on a piece of paper, but two of the digits are illegible. What you can read is the following (the units and hundreds digits are illegible).

57_3_

Fortunately, you know two facts about this number:

- It is divisible by both 4 and 9.
- All five digits are different.

Determine the number.

Let the digits be A and B . Then the number is

$$57030 + 100A + B.$$

Therefore

$$57030 + 100A + B \equiv 0 \pmod{4}$$

$$\Rightarrow 2 + B \equiv 0 \pmod{4}$$

$$\Rightarrow B \equiv 2 \pmod{4}$$

so B is 2 or 6.

Also,

$$57030 + 100A + B \equiv 0 \pmod{9}$$

since all powers of 10 are $1 \pmod{9}$:

$$5 + 7 + 3 + A + B \equiv 0 \pmod{9}$$

$$15 + A + B \equiv 0 \pmod{9}$$

$$A + B \equiv -15 \pmod{9}$$

$$\equiv 3 \pmod{9}.$$

So if $B=2$, then $A \equiv 1 \pmod{9}$, so $A=1$,
while if $B=6$, then $A \equiv -3 \pmod{9}$, so A is 6.

Since $A \neq B$, they can't be 6. So $A=1$ and $B=2$.

57132

(5 points)

(8) Suppose that a, e, f , and m are positive integers such that the following two congruences hold.

$$a^e \equiv 1 \pmod{m}$$

$$a^f \equiv 1 \pmod{m}$$

Prove that

$$a^{\gcd(e,f)} \equiv 1 \pmod{m}.$$

By the Euclidean algorithm, there are integers u & v st.

$$e \cdot u - f \cdot v = \gcd(e, f).$$

We can assume that u, v are positive (otherwise swap e and f).

Therefore:

$$a^{e \cdot u} \equiv a^{f \cdot v + \gcd(e, f)} \pmod{m}$$

$$\Rightarrow (a^e)^u \equiv (a^f)^v \cdot a^{\gcd(e, f)} \pmod{m}$$

$$\Rightarrow 1^u \equiv 1^v \cdot a^{\gcd(e, f)} \pmod{m}$$

$$\Rightarrow \underline{1 \equiv a^{\gcd(e, f)} \pmod{m}},$$

as desired.

(5 points)

(9) Solve the congruence

$$x^{23} \equiv 5 \pmod{29}.$$

Your answer should be in the form $x \equiv a \pmod{m}$, where a is between 0 and $m - 1$ inclusive.

(You may want to use the multiplication table on the last page.)

Hint. The answer will be congruent to 5^f for a well-chosen value of f .

IP $23f \equiv 1 \pmod{\varphi(29)}$, then $x^{23f} \equiv x^1 \pmod{29}$, so $5^f \equiv x$.
Since $\varphi(29) = 28$, we want an inverse of $23 \pmod{28}$.
Use the extended euclidean algorithm:

$$\begin{aligned} (28) \\ (23) \\ [5] &= (28) - (23) \\ [3] &= (23) - 4[5] \\ &= 5(23) - 4(28) \\ [1] &= 2 \cdot [3] - [5] \\ &= 11(23) - 9(28) \end{aligned}$$

So $11 \cdot 23 \equiv 1 \pmod{28}$, so we know that $x \equiv 5^{11} \pmod{29}$.
Use successive squaring: (w/ the mod 29 mult. table):

$$\begin{aligned} 5^1 &\equiv 5 \\ 5^2 &\equiv 5 \cdot 5 = 25 \\ 5^4 &\equiv 25 \cdot 25 \equiv 16 \\ 5^5 &\equiv 16 \cdot 5 \equiv 22 \\ 5^{10} &\equiv 22 \cdot 22 \equiv 20 \\ 5^{11} &\equiv 5 \cdot 20 \equiv 13 \end{aligned}$$

so $x \equiv 13 \pmod{29}$

(5 points)

- (10) Consider the rather large number $N = 2^{53^{69}}$ (Note that this is 2 raised to the power 53^{69} , not 2^{53} raised to the power 69.)
 (a) Find the remainder when N is divided by 4.

$$2^2 \mid N \text{ since } 53^{69} \geq 2. \text{ So } \boxed{N \equiv 0 \pmod{4}}.$$

- (b) Find the remainder when N is divided by 25.

$\varphi(25) = 20$, so we can first reduce $53^{69} \pmod{20}$ ($\gcd(2, 25) = 1$).
 similarly, $\varphi(20) = 8$, so we can first reduce $69 \pmod{8}$.

$$69 \equiv 5 \pmod{8}, \text{ so } 53^{69} \equiv 53^5 \pmod{20}$$

$$53 \equiv 13 \pmod{20}, \text{ so also } 53^5 \equiv 13^5 \pmod{20}$$

Now, $\pmod{20}$.

$$13^1 \equiv -7$$

$$13^2 \equiv 49 \equiv 9$$

$$13^4 \equiv 9^2 \equiv 81 \equiv 1$$

$$13^5 \equiv 13 \pmod{20}.$$

Thus $53^{69} \equiv 13 \pmod{20}$, hence $N \equiv 2^{13} \pmod{25}$.

By successive squaring,

$$2^1 \equiv 2 \pmod{25}$$

$$2^2 \equiv 4 \pmod{25}$$

$$2^3 \equiv 8 \pmod{25}$$

$$2^6 \equiv 64 \equiv 14 \pmod{25}$$

$$\equiv -11$$

$$2^{12} \equiv (-11)^2 \equiv 121 \pmod{25}$$

$$\equiv 21$$

$$2^{13} \equiv 2 \cdot 21 \equiv 42 \equiv 17 \pmod{25}.$$

$$\text{So } \boxed{N \equiv 17 \pmod{25}}.$$

- (c) From parts (a) and (b), deduce the last two digits (units digit and tens digit) of N .

From (a), $N = 4k$ for some k .

From (b), $4k \equiv 17 \pmod{25}$

$$19 \cdot 4k \equiv 19 \cdot 17 \pmod{25}$$

$$k \equiv (-6)(-8) \equiv 48 \equiv 23 \pmod{25}$$

$$\text{Hence } N = 4 \cdot (23 + 25h) = 92 + 100h,$$

$$\text{ie } N \equiv 92 \pmod{100}.$$

So the last two digits of N
 are $\boxed{92}$.

(6 points)

- (11) Alice has a message m , encoded as a number between 0 and 28 inclusive, which she wishes to communicate to you using ElGamal encryption¹. As part of your secret key, you know the following fact.

$$19^{10} \equiv 6 \pmod{29}$$

Alice has generated a number a , which she keeps secret, but she guarantees that the following two congruences are true.

$$19^a \equiv 7 \pmod{29}$$

$$m \cdot 6^a \equiv 10 \pmod{29}$$

From this information, recover the number m .

(You may wish to use the multiplication table on the last page.)

Hint. It is possible to compute m without computing the number a .

Since $6 \equiv 19^{10}$, it follows that

$$6^a \equiv (19^{10})^a \equiv (19^a)^{10} \equiv 7^{10} \pmod{29}.$$

By succ. squaring: (using the mult. table)

$$\begin{aligned} 7 &\equiv 7 \\ 7^2 &\equiv 20 \\ 7^4 &\equiv 23 \\ 7^5 &\equiv 23 \cdot 7 \equiv 16 \\ 7^{10} &\equiv 16 \cdot 16 \equiv 24 \end{aligned}$$

$$\text{so } 6^a \equiv 7^{10} \equiv 24 \pmod{29}.$$

Thus $m \cdot 24 \equiv 10 \pmod{29}$. Now find an inverse of $24 \pmod{29}$:

$$\begin{aligned} (29) \\ (24) \\ [5] &= (29) - (24) \\ [1] &= 5 \cdot [5] - (24) \\ &= 5(29) - 6 \cdot (24) \\ \Rightarrow 24 \cdot (-6) &\equiv 1 \pmod{29} \\ \text{ie. } 24 \cdot 23 &\equiv 1 \pmod{29}. \end{aligned}$$

$$\begin{aligned} \text{Thus} \\ m &\equiv 23 \cdot 10 \pmod{29} \\ &\equiv 27 \pmod{29} \text{ (using the chart)}. \end{aligned}$$

$$\boxed{m = 27}$$

(7 points)

¹You do not need any specific knowledge of ElGamal keys and encryption to solve the problem; the three congruences given are enough to solve for m .

Alt. sol'n: You can find that $a=20$ by guessing and checking. Then $6^a \equiv 6^{20} \equiv 24$ by succ. squaring, & proceed as before.

(12) Prove that the equation

$$a^2 + b^2 = 3$$

has no *rational* solutions (i.e. there are no two rational numbers a, b satisfying the equation).

↳ Suppose that $a^2 + b^2 = 3$, where $a, b \in \mathbb{Q}$. Then:

$$a = \frac{c}{d} \quad b = \frac{e}{d}, \quad c, d, e \in \mathbb{Z}.$$

(we can find a common denominator for a and b).

So

$$\frac{c^2}{d^2} + \frac{e^2}{d^2} = 3$$

$$\text{i.e. } c^2 + e^2 = 3d^2 \quad (\text{integers})$$

So $3d^2$ is a sum of two squares. But $3d^2$, when factored into primes, contains 3 an odd number of times (1 plus twice the number of times it occurs in d).

So $3d^2$ cannot be a sum of two integer squares, by Fermat's theorem on sums of two squares; this is a contradiction. \Leftarrow

So $a^2 + b^2 = 3$ has no rational solutions.

(7 points)