PMTH338 NUMBER THEORY

The tutorial questions contained in this booklet have mostly been selected from *Elementary Number Theory and its Applications* by Kenneth H. Rosen, 3rd ed. Addison Wesley. References to relevant sections from this text are included with each tutorial. If you have an earlier or later edition of this text, the chapter and section numbers may be different, but the corresponding material should be easy to locate.

Sample worked solutions for the tutorial questions are included in this booklet. Resist the temptation to refer to the the solution as soon as you encounter any difficulty. You will learn and remember more from perseverance, successful or not, than from simply following through a worked solution.

Some of the problems are straight forward and can be solved by elementary methods. The techniques introduced in the course will be useful to find shorter and more elegant solutions. Other problems have a simple and short solution if you understand and use the relevant concepts, but cannot be solved by naive methods. In this situation try to find out first what theorem or definition would prove useful. There are also some more challenging problems which require a good understanding of the material and an elaborate analysis of the problem, some times with separate investigation of distinct cases.

These questions and solutions have been prepared by Dr Mike Canfell (with minor changes and extensions by Dr Gerd Schmalz) at the School of Mathematics, Statistics and Computer Science, University of New England.

Printed at the University of New England
December, 2009

TUTORIAL PROBLEMS SET 1

1. Show that the natural numbers are not a group with respect to addition.

2. Using the definition, prove that for two integers a, b either $a < b$, or $a > b$, or $a = b$.

3. Show that a nonempty set of negative integers has a largest element.

4. Show that if a and b are positive integers, then there is a smallest positive integer of the form $a - bk, k \in \mathbb{Z}$.

5. Show that $a \mid b$ implies $|a| \mid |b|$.

6. Suppose a and b are positive integers such that $a \mid b$. Prove that $a \leq b$.

7. If a and b are nonzero integers such that $a \mid b$ and $b \mid a$ is it true that $a = b$?

8. Show that if a, b, c and d are integers with a and c nonzero such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.

9. Use the sieve of Eratosthenes to find all primes less than 200.

10. Find all primes that are the difference of the fourth powers of two integers.

11. Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.

12. Show that if a, b and c are integers such that $(a, b) = 1$ and $c \mid (a + b)$, then $(c, a) = (c, b) = 1$.

13. Use the Euclidean algorithm to find each of the following greatest common divisors.
    (a) $(45, 75)$ (b) $(102, 222)$

14. For each pair of integers in the previous problem, express the greatest common divisor of the integers as a linear combination of these integers.

15. Find the prime factorizations of each of the following integers.
    (a) 36 (b) 39 (c) 100 (d) 289 (e) 222 (f) 9999

16. Show that if a and b are positive integers with $a^3 \mid b^2$, then $a \mid b$.

17. Show if p is a prime and a is an integer with $p \mid a^2$, then $p \mid a$.

18. Show that $\sqrt{5}$ is irrational.

19. Find the prime factorization of 33776925.

20. Using Fermat's factorization method, factor each of the following positive integers.

    (i) 8051

    (ii) 11021

21. For each of the following linear diophantine equations, either find all solutions, or show that there are no integral solutions.

    (a) $2x + 5y = 11$

    (b) $21x + 14y = 147$

22. A student returning from Europe changes his French francs and Swiss francs into US money. If he receives \$17.06 and has received $19c$ for each French franc and $59c$ for each Swiss franc, how much of each type of currency did he exchange?

TUTORIAL PROBLEMS SET 2

1. Determine whether each of the following pairs of integers are congruent modulo 7.
   (a) $1, 15$ (d) $-1, 8$
   (b) $0, 42$ (e) $-9, 5$
   (c) $2, 99$ (f) $-1, 699$

2. For which positive integers m are each of the following statements true?

   (a) $27 \equiv 5 \pmod{m}$

   (b) $1000 \equiv 1 \pmod{m}$

   (c) $1331 \equiv 0 \pmod{m}$

3. Show that if a is an even integer, then $a^2 \equiv 0 \pmod 4$, and if a is an odd integer, then $a^2 \equiv 1 \pmod 4$.

4. Construct a table for addition modulo 6.

5. Construct a table for multiplication modulo 6.

6. Show by mathematical induction that if n is a positive integer then $4^n \equiv 1+3n \pmod 9$.

7. Find all solutions of the following linear congruences.

   (a) $3x \equiv 2 \pmod 7$,

   (b) $6x \equiv 3 \pmod 9$,

   (c) $17x \equiv 14 \pmod{21}$

8. For which integers c with $0 \le c < 30$ does the congruence $12x \equiv c \pmod{30}$ have solutions? When there are solutions, how many incongruent solutions are there?

9. Find an inverse modulo 17 of each of the following integers.
   (a) 4, (b) 5, (c) 7, (d) 16

10. Show that if $\bar{a}$ is an inverse of a modulo m and $\bar{b}$ is an inverse of b modulo m, then $\bar{a}\bar{b}$ is an inverse of ab modulo m.

11. What integers leave a remainder of one when divided by either 2 or 3?

12. Find all the solutions of the following system of linear congruences.

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

13. Show that if a, b and $c \neq 0$ are integers with $(a, b) = 1$, then there is an integer n such that $(an + b, c) = 1$. (Hint: Take n to be the product of all prime divisors of c that are not divisors of neither a nor b. This is a difficult problem.)

TUTORIAL PROBLEMS SET 3

1. Using Wilson's theorem, find the least positive residue of $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot$ modulo 7.

2. Using Fermat's little theorem, find the least positive residue of $2^{1000000}$ modulo 17.

3. Show that if p is an odd prime, then $2(p-3)! \equiv -1 \pmod{p}$.

4. Find a reduced residue system modulo each of the following integers.
   (a) 6 (b) 9 (c) 10

5. Use Euler's theorem to find the least positive residue of 3^{100000} modulo 35.

6. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1(\text{mod } ab)$, if a and b are relatively prime positive integers.

7. Determine whether the arithmetic function $f(n) = \text{log}n$ is multiplicative. Prove your answer.

8. Find the value of the Euler phi-function at each of the following integers.
   (i) 100 (ii) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.

9. For which positive integers n does $\phi(3n) = 3\phi(n)$?

10. Show that a positive n is composite if and only only if $\phi(n) \leq n - \sqrt{n}$.

11. Find the sum of the positive integer divisors of each of the following integers.
    (i) 1000 (ii) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

12. For which positive integers n is the sum of divisors of n odd?

13. If the ciphertext message produced by RSA cipher with key $(e, n) = (5, 2881)$ is 0603 2421 1470 2356, what is the plaintext message?

TUTORIAL PROBLEMS SET 4

1. Determine the following orders.
   (a) $\mathrm{ord}_5 2$ (b) $\mathrm{ord}_{10} 3$

2. Show that the integer 12 has no primitive roots.

3. Let $m = a^n - 1$, where a and n are positive integers. Show that $\mathrm{ord}_m a = n$ and conclude that $n \mid \phi(m)$.

4. Find the number of primitive roots for each of the following primes.
   (i) 19 (ii) 47

5. Find the least positive residue of the product of a set of $\phi(p-1)$ incongruent primitive roots modulo a prime p.

6. Let p be a prime of the form $p = 2q + 1$, where q is an odd prime. (a) How many primitive roots does p have?
   (b) Show that for any integer a with $1 < a < p - 1$, the number $p - a^2$ is a primitive root modulo p. (Thus in this situation we have a formula that provides primitive roots explicitely!)

7. Let p be an odd prime. Show that the congruence $x^4 \equiv -1 \pmod{p}$ has a solution if and only if p is the form $8k + 1$.

8. Prove that there are infinitely many primes of the form $8k+1$. (Hint: Assume that $p_1, p_2, \cdots p_n$ are the only primes of this form. Let $Q = (p_1, p_2 \cdots p_n)^4 + 1$. Show that Q must have an odd prime factor different than $p_1, p_2 \cdots p_n$, and then by Exercise 7, necessarily of the form $8k + 1$.

TUTORIAL PROBLEMS SET 5

1. Find all the quadratic residues of each of the following integers.
   (a) 3 (c) 13
   (b) 5 (d) 19

2. Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$.

3. Show that if p is an odd prime, then $\left(\frac{-2}{p}\right) = 1$ if $p \equiv 1$ or $3 \pmod{8}$, $\left(\frac{-2}{p}\right) = -1$ if $p \equiv -1$ or $-3 \pmod{8}$.

4. Find all solutions of the congruence $x^2 \equiv 1 \pmod{15}$.

5. Evaluate each of the following Legendre symbols.
   (a) $\left(\frac{3}{53}\right)$, (b) $\left(\frac{7}{79}\right)$, (c) $\left(\frac{15}{101}\right)$

6. Show that there are infinitely many primes of the form $5k + 4$. (Hint: Let n be a positive integer and form $Q = 5(n!)^2 - 1$. Show that Q has a prime divisor of the form $5k + 4$ greater than n. To do this, use the law of quadratic reciprocity to show that if a prime p divides Q, then $\left(\frac{p}{5}\right) = 1$).

7. Evaluate each of the following Jacobi symbols.
   (a) $\left(\frac{5}{21}\right)$, (b) $\left(\frac{27}{101}\right)$

8. For which positive integers n that are relatively prime to 30 does the Jacobi symbol $\left(\frac{30}{n}\right)$ equal 1?

TUTORIAL PROBLEMS SET 6

1. Find all
   (a) Primitive Pythagorean triples x, y, z with $z \leq 40$.
   (b) Pythagorean triples x, y, z with $z \leq 40$.
2. Show that if x, y, z is a Pythagorean triple and n is an integer $n > 2$, then $x^n + y^n \neq z^n$.
3. Suppose that m and n are both sums of two squares. Show that mn is also the sum of two squares.
4. Solve the Diophantine equation $x^2 + xy + y^2 = x^2 y^2$.

NUMBER THEORY SOLUTIONS
TUTORIAL PROBLEMS SET 1.

1. Numbers a with $a > 0$ have no (additive) inverse in $\mathbb{N}$.

2. $a < b$ is equivalent to $b - a = x > 0$, $a > b$ is equivalent to $a - b = -x > 0$, i.e. $x < 0$. But x can only be positive (in $\mathbb{N}$ and not 0), or negative (in $-\mathbb{N}$ and not 0), or 0.

3. Let S be a nonempty set of negative integers. Consider the set $T = \{-s : s \in S\}$. Then T is a nonempty set of positive integers and by the well-ordering principle has a least element $-s_0$ for some $s_0 \in S$. Then $-s_0 \leq -s$ for every $s \in S$. Hence $s_0 \geq s$ for every $s \in S$. This means that s_0 is the greatest element of S.

4. Let a and b be positive integers and let

   $$S = \{n : n \text{ is a positive integer and } n = a - bk \text{ for some } k \in \mathbb{Z}\}$$

   Now S is nonempty since $a + b = a - b(-1)$ is in S. By the well-ordering principle, S has a least element.

5. $a \mid b$ means $a \neq 0$ and $ac = b$ for some integer c. If a, b are both non-negative then

   $$|a|c = ac = b = |b|.$$

   If $a < 0$ and $b > 0$ then

   $$|a|(-c) = -a(-c) = b = |b|.$$

   If $a > 0$ and $b < 0$ then

   $$|a|(-c) = a(-c) = -b = |b|.$$

   and if $a < 0$ and $b < 0$ then

   $$|a|c = -ac = -b = |b|.$$

6. If $a \mid b$ then $ac = b$ with $c \geq 1$. Hence $a + (c-1)a = b$ where $c - 1 \geq 0$. By definition then $a \leq b$.

7. For $a \neq 0$ we have $a \mid -a$ and $-a \mid a$ but $a \neq -a$. However it is true that $a \mid b$ and $b \mid a$ implies $a = b$ if both numbers are positive, since according to the previous problem then $a \leq b$ and $b \leq a$.

8. Suppose $a \mid b$ and $c \mid d$ with $a \neq 0$, $c \neq 0$. Then $b = as, d = ct$ for integers s, t. Hence $bd = acst$ and therefore $ac \mid bd$.

9. We first write down all the integers from 2 to 200.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	49	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

We first cross out all multiples of 2 (but not 2 itself). This means that we cross out all even numbers from 4 onwards, and we could have saved some effort by just writing down the even numbers in the first place. Then we cross out all multiples of 3 (but not 3 itself). The numbers removed in this step are 9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99, 105, 111, 117, 123, 129, 135, 141, 147, 153, 159, 165, 171, 177, 183, 189, 195. Then starting with $25 = 5^2$ we remove multiples of 5. These numbers are 25, 35, 55, 65, 85, 95, 115, 125, 145, 155, 175, 185. Then starting with $49 = 7^2$ we remove multiples of 7. These numbers are 49, 77, 91, 119, 133, 161. Then starting with $121 = 11^2$ we remove multiples of 11. These numbers are 121, 143, 187. Finally, starting with $169 = 13^2$ we remove multiples of 13. The only such number is 169.

Since $17 > \sqrt{200}$ we do not need to use any more primes. The integers remaining are the primes below 200. These are

$$\begin{array}{rrrrrrrr}
2, & 3, & 5, & 7, & 11, & 13, & 17, & 19 \\
23, & 29, & 31, & 37 & & & & \\
41, & 43, & 47, & 53, & 59, & & & \\
61, & 67, & 71, & 73, & 79, & & & \\
83, & 89, & 97 & & & & & \\
101, & 103, & 107, & 109, & 113 & & & \\
127 & 131, & 137, & 139 & & & & \\
149, & 151, & 157 & & & & & \\
163, & 167, & 173, & 179 & & & & \\
181, & 191, & 193, & 197, & 199 & & &
\end{array}$$

10. Suppose p is a prime and

$$\begin{aligned}
p &= n^4 - m^4 \\
&= (n^2 - m^2)(n^2 + m^2) \\
&= (n - m)(n + m)(n^2 + m^2)
\end{aligned}$$

for integers m, n, where $n > m$.

Since p is prime, its only factorization using positive integers is $p = 1.p$. Hence p is not prime since it is divisible by the distinct integers $n-m, n+m, n^2+m^2$.

11. Suppose p is prime and $p = n^3+1 = (n+1)(n^2-n+1)$. Then either $n+1 = 1$ and $n = 0$ or $n^2-n+1 = 1$ and $n = 0$ or 1. The only case when p is prime is when $n = 1$ and $p = 2$.

12. Suppose $(a, b) = 1$ and $c \mid (a+b)$. Then $sa + tb = 1$ for some integers s, t. Also $a + b = ck$. Hence $sa + t(ck - a) = 1$ i.e. $(s-t)a + tkc = 1$ which shows that $(a, c) = 1$. Also $s(ck - b) + tb = 1$ i.e. $(t-s)b + skc = 1$ which shows that $(b, c) = 1$.

13. (a)

$$\begin{aligned} 75 &= 45 + 30 \\ 45 &= 30 + 15 \\ 30 &= 2 \cdot 15 \end{aligned}$$

Hence $(75, 45) = 15$.

(b)

$$\begin{aligned} 222 &= 2 \cdot 102 + 18 \\ 102 &= 5 \cdot 18 + 12 \\ 18 &= 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

Hence $(222, 102) = 6$.

14. Referring to the working in the previous question, and working backwards, we get

(a)

$$\begin{aligned} 15 &= 45 - 30 \\ &= 45 - (75 - 45) \\ &= 2 \cdot 45 - 75 \end{aligned}$$

(b)

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (102 - 5 \cdot 18) \\ &= 6 \cdot 18 - 102 \\ &= 6(222 - 2 \cdot 102) - 102 \\ &= 6 \cdot 222 - 13 \cdot 102 \end{aligned}$$

Hence $(-1)75 + 2 \cdot 45 = 1$ and $222(6) + (-13)102 = 6$.

15. (a) $36 = 2^2 \cdot 3^2$

    (b) $39 = 3 \cdot 13$

    (c) $100 = 2^2 \cdot 5^2$

    (d) $289 = 17^2$

    (e) $222 = 2 \cdot 111 = 2 \cdot 3 \cdot 37$

    (f) $9999 = 9 \cdot 1111 = 3^2 \cdot 11 \cdot 101$

16. Suppose $a^3 \mid b^2$. Then $b^2 = ka^3$ for some integer k. Let $p_1, p_2, \cdots p_n$ be the primes which occur in the factorizations of a, b and k. We can write

$$\begin{aligned} k &= p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n} \\ a &= p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n} \\ b &= p_1^{u_1} p_2^{u_2} \cdots p_n^{u_n} \end{aligned}$$

(Some of the s_i, t_i, u_i may be 0). Since $b^2 = ka^3$ we have

$$2u_i = s_i + 3t_i \qquad \text{for } i = 1, \cdots, n.$$

Hence $t_i = \frac{2}{3}u_i - \frac{s_i}{3} \leq u_i$. Thus $p^{t_i} \mid p^{u_i}$ for $i = 1, \cdots, n$ and it follows that $a \mid b$.

17. Let $p \mid a^2$. Suppose $p \nmid a$. Then $(a, p) = 1$ so there exist integers s and t such that $as + pt = 1$. Then multiplying through by a we get $a^2 s + apt = a$. Since $p \mid a^2, p$ divides the LHS hence $p \mid a$. This is a contradiction. We conclude that $p \mid a$.

18. Suppose $\sqrt{5} = \frac{a}{b}$. After cancelling any common factor, we can assume that a and b are relatively prime integers with $b \neq 0$. Then $5 = \frac{a^2}{b^2}$ or $a^2 = 5b^2$. Since 5 is prime and $5 \mid a^2$, it follows that $5 \mid a$. Hence $a = 5c$ for some integer c. But $(5c)^2 = 5b^2$ so $5c^2 = b^2$. Hence $5 \mid b^2$ and from this it follows that $5 \mid b$.

    Since $(a, b) = 1$ we know that 5 cannot divide both a and b.

    This is a contradiction. We conclude that $\sqrt{5}$ is irrational.

19.

$$\begin{aligned} 33776925 &= 3(11258975) = 3 \cdot 5(2251795) \\ &= 3 \cdot 5^2(450359) = 3 \cdot 5^2 \cdot 7(64337) \\ &= 3 \cdot 5^2 \cdot 7^2(9191) = 3 \cdot 5^2 \cdot 7^3(1313) \\ &= 3 \cdot 5^2 \cdot 7^3 \cdot 13 \cdot 101 \end{aligned}$$

20. (i) $n = 8051$, and $89 < \sqrt{n} < 90$.

We start with $t = 90$.

$$90^2 - n = 8100 - 8051 = 49 = 7^2$$

Hence

$$\begin{aligned} n &= 90^2 - 7^2 = (90+7)(90-7) \\ 8051 &= 83 \cdot 97 \end{aligned}$$

[If $t = 90$ did not work we would have tried $t = 91, t = 92, \cdots$ until a perfect square arose.]

(ii) $\sqrt{11021} = 104.98$ so take $t = 105$.

$$\begin{aligned} 105^2 - 11021 &= 4 = 2^2 \text{ so} \\ 11021 &= 105^2 - 2^2 \\ &= 103 \cdot 107 \end{aligned}$$

21. (a) $2x + 5y = 11$.

Since $(a, b) = (2, 5) = 1$ there are infinitely many solutions. We first find a solution of $2x + 5y = 1$. Observe that $x = -2,\ y = 1$ is one solution. Hence on multiplying these terms by 11, we see that one solution of $2x + 4y = 11$ is $x_0 = -22,\ y_0 = 11$. Using the general theory we see that all solutions are given by $x = -22 + 5n,\ y = 11 - 2n$.

[Remark: you may have used a different (x_0, y_0) for your solution].

(b) $21x + 14y = 147$

Here $(a, b) = (21, 14) = 7$ and $7 \mid 147$ so there are infinitely many solutions. We first solve $21x + 14y = 7$. One solution is $(1, -1)$ so one solution of $21x + 14y = 147$ is $x_0 = 21$ $y_0 = -21$. The general solution is then $x = 21 + \frac{14}{7}n = 21 + 2n,\ y = -21 - \frac{21}{7}n = -21 - 3n$.

22. Let x be the number of French francs and y the number of Swiss francs exchanged. We have to solve

$$19x + 59y = 1706$$

Since $(19, 59) = 1$ there are infinitely many solutions, but we only want solutions with $x \geq 0, y \geq 0$. By the Euclidean algorithm, we find that one solution of $19x+59y = 1$ is $x = 28,\ y = -9$ so on multiplying by 1706 we see that one solution $19x+59y = 1706$ is $x_0 = 28{\cdot}17{-}6 = 47768$ and $y_0 = -9{\cdot}1706 = -15354$. All solutions are given by $x = 47768 + 59n,\ y = -15354 - 19n$.

Now $x \geq 0,\ y \geq 0$ so

$$\begin{aligned} -15354 - 19n \geq 0 &\qquad \text{i.e. } n \leq \frac{-15354}{19} = -808.1 \\ \text{and } \ 47768 + 59n \geq 0 &\qquad \text{i.e. } n \geq \frac{-47768}{59} = -809.6 \end{aligned}$$

Hence $n = -809$, and

$$\begin{aligned} x &= 47768 - 59 \cdot 809 = 37 \\ y &= -15354 + 19 \cdot 809 = 17 \end{aligned}$$

So he had 37 French francs and 17 Swiss francs.

NUMBER THEORY SOLUTIONS
TUTORIAL PROBLEMS SET 2.

1. (a) $1 \equiv 15 \pmod 7$ since $7 \mid (15-1) = 14$

   (b) $0 \equiv 42 \pmod 7$ since $7 \mid (42-0) = 42$

   (c) $2 \not\equiv 99 \pmod 7$ since $7 \nmid (99-2) = 97$

   (d) $-1 \not\equiv 8 \pmod 7$ since $7 \nmid (8-(-1) = 9$

   (e) $-9 \equiv 5 \pmod 7$ since $7 \mid (5-(-9)) = 14$

   (f) $-1 \equiv 699 \pmod 7$ since $7 \mid (699-(-1)) = 700$

2. (a) $27 \equiv 5$ (mod m) iff $m \mid (27-5)$ i.e. $m \mid 22$. Hence $m = 1, 2, 11$ or 22.

   (b) $1000 \equiv 1$ (mod m) iff $m \mid 999$. Now $999 = 3^3.37$ so m can be any of 1, 3, 9, 27, 37, 111, 333, 999.

   (c) $1331 \equiv 0$ (mod m) iff $m \mid 1331$. Now $1331 = 11^3$ so m can be any of 1, 11, 121, 1331.

3. If a is even, then $a = 2b$ for some integer b. Hence $a^2 = 4b^2$ and so $a^2 \equiv 0$ (mod 4).

   If a is an odd integer, then $a = 2b+1$ for some integer b. Hence $a^2 = 4b^2+4b+1$ and so $a^2 \equiv 1 \pmod 4$.

4. Addition modulo 6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

5. Multiplication modulo 6

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

6. Let $P(n)$ be the statement $4^n \equiv 1 + 3n \pmod 9$.

(a) $P(1)$ is true since it is the statement $4 \equiv 1 + 3 \pmod 9$.

(b) Suppose $P(k)$ is true i.e. $4^k \equiv 1 + 3k \pmod 9$. Then

$$\begin{aligned} 4^{k+1} &= 4 \cdot 4^k \equiv 4(1+3k) \pmod 9 \\ &\equiv 4 + 12k = 1 + 3(k+1) + 9k \\ &\equiv 1 + 3(k+1) \pmod 9 \end{aligned}$$

Hence $P(k+1)$ is true.

By induction, $P(n)$ is true for all positive integers n.

7. (a) $3x \equiv 2 \pmod 7$

Since $(3,7) = 1$ there is a unique solution (mod 7).

Method 1 Since there are only 7 possibilities, we can inspect each one. Now (modulo 7) $3 \cdot 0 \equiv 0$, $3 \cdot 1 \equiv 3$, $3 \cdot 2 \equiv 6$, $3 \cdot 3 \equiv 2$. Hence $x = 3$ is one solution. All solutions are given by $x \equiv 3 \pmod 7$.

Method 2 (Euclidean algorithm). We solve $3x + 7y = 2$ for integers x and y (because then $3x \equiv 2 \pmod 7$ if $3x + 7y = 2$). To do this we first solve $3x + 7y = 1$. Now $7 = 2 \cdot 3 + 1$ or

$$3(-2) + 1 \cdot 7 = 1.$$

Multiplying by 2, $3(-4) + 2 \cdot 7 = 2$.

Hence $x = -4,\ y = 2$ is a solution. The solutions of $3x \equiv 2 \pmod 7$ are then $x \equiv -4 \pmod 7$, that is, $x \equiv 3 \pmod 7$.

Method 3 We note by inspection that 5 is an inverse of 3 modulo 7. On multiplying the congruence by 5 we get

$5 \cdot 3x \equiv 5 \cdot 2$, (mod 7), that is $x \equiv 3 \pmod 7$.

(b) $6x \equiv 3 \pmod 9$.

Since $(6,9) = 3$ and $3 \mid 3$ there are 3 distinct solutions mod 9. By inspection, one solution is $x_o = 2$. Adding multiples of 3 to 2 we get the other solutions 5 and 8. All solutions are given by $x \equiv 2, 5, 8 \pmod 9$.

(c) $17x \equiv 14 \pmod{21}$

Since $(17, 21) = 1$ there is a unique solution modulo 21. Solving $17x + 21y = 1$ by the Euclidean algorithm we get a solution $x = 5, y = -4$. Hence one solution of $17x + 21y = 14$ is $x = 5 \cdot 14$, $y = -4 \cdot 14$. All solutions are given by $x \equiv 70 \pmod{21}$, that is, $x \equiv 7 \pmod{21}$.

8. $12x \equiv c \pmod{30}$

Since $(12, 30) = 6$ there are solutions if and only if $6 \mid c$. For $0 \le c < 30$ the possibilities are $c = 0, 6, 12, 18, 24$. In each case there are 6 incongruent solutions modulo 30.

9. (a) $4x \equiv 1 \pmod{17}$.

We solve $4x + 17y = 1$ using the Euclidean algorithm.

$$17 = 4 \cdot 4 + 1 \quad \text{so} \quad (-4)4 + 17 = 1$$

$$\begin{aligned} \text{Solution:} \quad & x \equiv -4 \pmod{17} \\ \text{i.e.} \quad & x \equiv 13 \pmod{17}. \end{aligned}$$

(b) $5x \equiv 1 \pmod{17}$. Solution $x \equiv 7 \pmod{17}$.

(c) $7x \equiv 1 \pmod{17}$. Solution $x \equiv 5 \pmod{17}$.

(Note that 7 and 5 are inverses of each other modulo 17).

(d) $16x \equiv 1 \pmod{17}$. Solution $x \equiv 16 \pmod{17}$.

(Note that if p is a prime, then 1 and $p - 1$ are their own inverses (mod p)).

10. Suppose $a\bar{a} \equiv 1$ (mod m) and $b\bar{b} \equiv 1$ (mod m). Then $1 \equiv (a\bar{a})(b\bar{b}) = (ab)(\bar{a}\bar{b})$ (mod m) so $\bar{a}\bar{b}$ is an inverse of ab (mod m).

11. We want the integers x which satisfy the system

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{3} \end{aligned}$$

By the Chinese Remainder Theorem, there is a unique solution modulo $2 \cdot 3$, since $(2, 3) = 1$. Clearly $x = 1$ is one solution. The general solution is $x \equiv 1 \pmod{6}$.

12.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

By the Chinese Remainder Theorem, there is a unique solution (mod 210) since the moduli 2, 3, 5, 7 are pairwise relatively prime. We construct a solution using the method in the proof of the Chinese Remainder Theorem.

Let $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and

$$\begin{aligned} M_1 &= \frac{210}{2} = 105 & \qquad M_3 &= \frac{210}{5} = 42 \\ M_2 &= \frac{210}{3} = 70 & \qquad M_4 &= \frac{210}{7} = 30 \end{aligned}$$

We have $a_1 = a_2 = 0$ $a_3 = 1$ $a_4 = 6$ $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$.

From theory, one solution is

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \\ &= a_3M_3y_3 + a_4M_4y_4 \end{aligned}$$

where $42y_3 \equiv 2y_3 \equiv 1 \pmod 5$, $30y_4 \equiv 2y_4 \equiv 1 \pmod 7$.

Solving these two congruences, we find $y_3 = 3$ and $y_4 = 4$.

Hence $x = 1 \cdot 42 \cdot 3 \quad + \quad 6 \cdot 30 \cdot 4 = 846$.

The general solution is $x \equiv 846 \pmod{210}$ or $x \equiv 6 \pmod{210}$ since $846 - 4 \cdot 210 = 6$.

13. Since $(a, b) = 1$ there is no prime which divides both a and b. Given c consider its prime factorization. The factors can be classified into three types:

    (1) factors which divide a but not b.

    (2) factors which divide b but not a.

    (3) factors which divide neither a nor b.

    Let $c = p_1^{\alpha_1} \cdots p_k^{\alpha_k}\ q_1^{\beta_1} \cdots q_l^{\beta_l} r_1^{\gamma_1}\ \cdots\ r_m^{\gamma_m}$ where $p_i \mid a,\ q_i \mid b$ and $r_i \nmid a,\ r_i \nmid b$.

    Let $n = r_1 \cdots r_m$ (if there are no factors of the type r_i we put $n = 1$).

    We now show $(a + nb, c) = 1$.

    Since $p_i \mid a$, we cannot have $p_i \mid (a + nb)$ (otherwise we would have $p_i \mid nb$ and since $(n, p_i) = 1$ this would mean $p_i \mid b$ contradicting $(a, b) = 1$).

    Similarly we cannot have $q_i \mid (a + nb)$ (for then we would have both $q_i \mid a$ and $q_i \mid b$, contradicting $(a, b) = 1$).

    Since $r_i \mid n$ we cannot have $r_i \mid (a + nb)$, (since $r_i \nmid a$).

    Hence no prime can divide both $a + nb$ and c, so

    $$(a + nb,\ c) = 1.$$

NUMBER THEORY SOLUTIONS
TUTORIAL PROBLEMS SET 3.

1. Note that $7 + n \equiv n \pmod 7$ so

$$\begin{aligned} 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod 7 \\ &\equiv -1 \pmod 7 \text{ by Wilson's theorem} \\ &\equiv 6 \pmod 7 \end{aligned}$$

i.e. 6 is the least positive residue mod 7.

2. With $p = 17$, $a = 2$ we have $p \nmid a$. by Fermat's Little Theorem,

$$2^{16} \equiv 1 \pmod{17}.$$

Also $1000000 = 62500 \cdot 16$. Hence $2^{1000000} = (2^{16})^{62500} \equiv 1 \pmod{17}$.

3. Let p be a prime where $p \neq 2$. Then by Wilson's theorem

$$(p-1)! \equiv -1 \quad (\text{mod p}).$$

Now

$$\begin{aligned} (p-1)! &= (p-1)(p-2)(p-3)! \\ &\equiv (-1)(-2)(p-3)! \quad (\text{mod p}) \\ &\equiv 2(p-3)! \quad (\text{mod p}) \end{aligned}$$

Hence $2(p-3)! \equiv -1$ (mod p).

4. (a) 1, 5
   (b) 1, 2, 4, 5, 7, 8
   (c) 1, 3, 7, 9

5. $(3, 35) = 1$ and $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$.

Hence $3^{24} \equiv 1 \pmod{35}$ by Euler's Theorem. Now

$$100000 = 4166 \cdot 24 + 16$$

so $3^{100000} = (3^{24})^{4166} 3^{16} \equiv 3^{16} \pmod{35}$

Now

$$\begin{aligned} 3^2 &\equiv 9 \pmod{35} \\ 3^4 &\equiv 81 \equiv 11 \text{ mod } 35) \\ 3^8 &\equiv 11^2 = 121 \equiv 16 \pmod{35} \\ 3^{16} &\equiv 16^2 \equiv 11 \pmod{35} \\ \text{So} \quad 3^{100000} &\equiv 11 \pmod{35} \end{aligned}$$

6. Suppose $(a,b)=1$. Then

$$a^{\phi(b)} \equiv 1 \pmod{b} \quad \text{and} \quad b^{\phi(a)} \equiv 1 \pmod{a}.$$

Hence $a^{\phi(b)} = 1 + k_1 b,\ b^{\phi(a)} = 1 + k_2 a$ for $k_1, k_2 \in \mathbb{Z}$.

Rearranging and multiplying gives

$$\begin{aligned} (a^{\phi(b)}-1)(b^{\phi(a)}-1) &= k_1k_2ab \\ a^{\phi(b)}b^{\phi(a)} - b^{\phi(a)} - a^{\phi(b)} + 1 &= k_1k_2ab \\ a^{\phi(b)} + b^{\phi(a)} - 1 &= a^{\phi(b)}b^{\phi(a)} - k_1k_2ab \\ &\equiv 0 \pmod{ab} \end{aligned}$$

(since $a^{\phi(b)}b^{\phi(a)}$ contains a factor ab).

7. $f(n) = \log n$ is not multiplicative since $\log(mn) = \log m + \log n$ is not equal to $(\log m)(\log n)$ in general. A specific counter example is given by $m = 2$, $n = e$. Then $\log(2e) = \log 2 + \log e = 1.69$ to 2 decimal places. However $(\log 2)(\log e) = 0.69$ to 2 decimal places.

8. (i)

$$\begin{aligned} \phi(100) &= \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) \\ &= (2^2-2)(5^2-5) = 40 \end{aligned}$$

(ii)

$$\begin{aligned} \phi(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13) &= \phi(2)\phi(3)\phi(5)\phi(7)\phi(11)\phi(13) \\ &= 1\cdot 2\cdot 4\cdot 6\cdot 10\cdot 12 = 5760 \end{aligned}$$

9. If $(3,n)=1$ then

$$\phi(3n) = \phi(3)\phi(n) = 2\phi(n) \neq 3\phi(n).$$

If $(3,n) \neq 1$ then $3 \mid n$. Put $n = 3^\alpha m$ where $(3,m)=1$. Then

$$\begin{aligned} \phi(3n) &= \phi(3^{\alpha+1}m) = \phi(3^{\alpha+1})\phi(m) = (3^{\alpha+1}-3^\alpha)\phi(m) \\ 3\phi(n) &= 3\phi(3^\alpha m) = 3\phi(3^\alpha)\phi(m) = 3(3^\alpha - 3^{\alpha-1})\phi(m) = \phi(3n). \end{aligned}$$

Hence $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.

10. If n is a prime, $n = p$ say, then $\phi(n) = p - 1 > p - \sqrt{p}$ so $\phi(n) \not\leq n - \sqrt{n}$.

If n is composite, we can write out its prime factorization as

$$\begin{aligned} n &= p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k} \text{ where } p_1 \text{ is the smallest prime factor.} \\ \text{Hence } \phi(n) &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right) \\ &< n\left(1-\frac{1}{p_1}\right) < n\left(1-\frac{1}{\sqrt{n}}\right) \\ \phi(n) &< \left(n-\frac{n}{\sqrt{n}}\right) = n-\sqrt{n}. \end{aligned}$$

(Note that we have used $p_1 \leq \sqrt{n}$). Hence n composite if and only if $\phi(n) \leq n-\sqrt{n}$.

11. (i) $1000 = 8\cdot 125 = 2^3\cdot 5^3$.

Using the formula with $p_1 = 2, p_2 = 5$ we have $\sigma(1000) = \frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}$.

$$\begin{aligned} &= \frac{2^4-1}{2-1}\cdot\frac{5^4-1}{5-1} = (16-1)\left(\frac{625-1}{5-1}\right) \\ &= 15\cdot\frac{624}{4} = 2340. \end{aligned}$$

(ii)

$$\begin{aligned} \sigma(2\cdot 3\cdot 5\cdot 7\cdot 11) &= \sigma(2)\sigma(3)\sigma(5)\sigma(7)\sigma(11) \\ &= 3\cdot 4\cdot 6\cdot 8\cdot 12 = 6912. \end{aligned}$$

12. Let $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ be the prime factorization of n. Then

$$\sigma(n) = \sigma\left(p_1^{a_1}\right)\sigma\left(p_2^{a_2}\right)\cdots\sigma\left(p_s^{a_s}\right)$$

where $\sigma(p^a) = 1+p+\cdots+p^a$.

If $p = 2$, each p^i is even so $\sigma(2^a)$ is odd. If $p \geq 3$, each term in the sum

$$\sigma(p^a) = 1+p+\cdots+p^a$$

is odd. Hence $\sigma(p^a)$ is even if a is odd and $\sigma(p^a)$ is odd if a is even. If any term $\sigma(p^a)$ is even then $\sigma(n)$ is even. Hence $\sigma(n)$ is odd if and only if, whenever p is an odd prime factor of n, the index a is even. This is the case when n can be written in the form $n = 2^k m^2$ where m is an odd integer.

13. We first find the decoding key. Using our list of primes < 200, we find that the first prime which divides 2881 is 43, and then $2881 = 43\cdot 67$.

Hence $\phi(2881) = 42\cdot 66 = 2772$. We note that $(5, 2772) = 1$. Now

$$\begin{aligned} 2772 &= 5\cdot 554+2 \\ 5 &= 2\cdot 2+1 \\ \text{So } 1 &= 5-2\cdot 2 \\ &= 5-2(2772-5\cdot 554) \\ &= 5\cdot 1109-2772\cdot 2 \end{aligned}$$

Since $5 \cdot 1109 \equiv 1 \pmod{2772}$ we take $d = 1109$. Also $n = 2881$ so the decoding key is $(1109, 2881)$.

(Note that when n is small we are easily able to 'crack' the code because it is easy to factorize n. In practice the code is only secure for n very large). We now use NUMBERS to perform the reductions modulo 2881

$$\begin{aligned}
(0603)^{1109} &\equiv 0603 \pmod{2881} \longrightarrow \text{GD}\\
(2421)^{1109} &\equiv 0024 \pmod{2881} \longrightarrow \text{AY}\\
(1470)^{1109} &\equiv 1200 \pmod{2881} \longrightarrow \text{MA}\\
(2356)^{1109} &\equiv 1904 \pmod{2881} \longrightarrow \text{TE}
\end{aligned}$$

Hence the message is

GDAYMATE

NUMBER THEORY SOLUTIONS TUTORIAL PROBLEMS SET 4.

1. (a)

$$\begin{aligned} 2^1 &\equiv 2 \pmod 5,\ 2^3 \equiv 3 \pmod 5 \\ 2^2 &\equiv 4 \pmod 5,\ 2^4 \equiv 1 \pmod 5 \end{aligned}$$

Hence $\mathrm{ord}_5 2 = 4$.

(b) Note that $\phi(10) = \phi(2)\phi(5) = 4$ and the divisors of 4 are $1, 2, 4$. The order of 3 mod 10 has to be one of $1, 2, 4$, so we can just test these numbers.

$$3^1 \equiv 3 \pmod{10},\quad 3^2 \equiv 9 \pmod{10},\quad 3^4 \equiv 1 \pmod{10}.$$

Hence $\mathrm{ord}_{10} 3 = 4$.

2. $\phi(12) = 4$. Also (a,12 $= 1$) for $a = 1, 5, 7, 11$. Now

$$1^1 \equiv 1,\ 5^2 \equiv 1,\ 7^2 \equiv 1,\ 11^2 \equiv 1 \pmod{12}.$$

In no case does $(a, 12) = 1$ and $\mathrm{ord}_{12} a = 4$. Hence 12 has no primitive roots.

3. Assume $a > 0, n > 0, m > 0$. Since $(-1)m + a(a^{n-1}) = 1$ we have $(a, m) = 1$. Let $t = \mathrm{ord}_m a$.

Now $a^n \equiv 1 \pmod m$ so $t \mid n$.

Also $a^t \equiv 1 \pmod m$ so $a^t - 1 = km$ for some $k \geq 1$.

Hence $a^t - 1 = k(a^n - 1) \geq a^n - 1$.

Hence $a^t \geq a^n$ and $t \geq n$.

Since $t \mid n$ and $t \geq n$ we have $t = n$.

Finally $n \mid \phi(m)$, since $\mathrm{ord}_m a \mid \phi(m)$.

4. (i) 19 has $\phi(18) = \phi(2)\phi(3^2) = 6$ primitive roots.

(ii) 47 has $\phi(46) = \phi(2)\phi(23) = 22$ primitive roots.

5. Let p be a prime and let r be a primitive root of p. Then the inverse $r^{-1} = r^{p-2}$ is a primitive root as well. Thus we can group the primitive roots in pairs of mutually inverse roots whenever r and r^{-1} are different from each other.

Let us investigate when r and r^{-1} can coincide.

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

implies $r \equiv \pm 1 \pmod{p}$ which are not primitive roots if $p > 3$. So for $p > 3$ the primitve roots group in pairs of mutually inverse primitive roots and their total product is congruent to 1 modulo p.

If $p = 2$ there is only one primitve root, namely 1. So the least positive residue of the product of all primitive roots is again 1 modulo p.

If $p = 3$ the only primitive root is $-1 \equiv 2$. In this case the least positive residue of the product of all primitive roots equals 2.

6. (a) There are $\phi(\phi(p))$ primitive roots. We have $\phi(p) = p - 1 = 2q$. Hence there are $\phi(2q) = (2-1)(q-1) = q - 1$ primitive roots.

   (b) Let $q > 2$, $p = 2q + 1, 1 < a < p - 1$. Note that $(p - a^2, p) = 1$ since $p \nmid a$. Now, by Fermat's Little Theorem $(p - a^2)^{p-1} \equiv 1 \pmod{p}$. Hence $t = \text{ord}(p - a^2)$ divides $p - 1 = 2q$. Hence t must be one of $1, 2, q, 2q$ since q is prime and these numbers are the only divisors of $2q$. We show that the first three possibilities cannot occur.

   (i) Suppose $t = 1$. Then $p - a^2 \equiv 1 \pmod{p}$ and so

   $$\begin{aligned} a^2 &\equiv -1 \pmod{p}. \text{ Hence} \\ a^4 &\equiv 1 \pmod{p}. \end{aligned}$$

   We claim that $\text{ord}_p\, a = 4$. The order has to divide 4 and it cannot be 2 since if $a^2 \equiv 1$ (mod p) (as well as $a^2 \equiv -1$ mod p) we would have on subtracting, $2 \equiv 0$ mod p which is impossible since $p > 2$.

   Hence $\text{ord}_p a = 4$ so $4 \mid \phi(p) = p - 1$ i.e. $4 \mid 2q$ whence $2 \mid q$ which is impossible since q is prime.

   We conclude that the case $t = 1$ cannot occur.

   (ii) If $t = 2$ we have $(p - a^2)^2 \equiv 1$ (mod p) and again $a^4 \equiv 1$ (mod p). Again we cannot have $a^2 \equiv 1$ (mod p) for this would mean

   $$p \mid (a^2 - 1) = (a - 1)(a + 1)$$

   which would give $a \equiv 1$ (mod p) or $a \equiv -1$ (mod p). Both of these possibilities are ruled out by the choice of a.

   The rest of the argument is the same as for (i).

   (iii) If $t = q$ we have $(p - a^2)^q \equiv 1$ (mod p). Since q is odd, this means $-a^{2q} \equiv 1$ (mod p). But $a^{2q} \equiv 1$ (mod p) so we get $2 \equiv 0$ (mod p) which again is an impossibility.

   We conclude that $t = 2q = p - 1$ and therefore $p - a^2$ is a primitive root.

7. Suppose p is an odd prime of the form $p = 8k + 1$. Then $8 \mid (p - 1)$, that is, $8 \mid \phi(p)$. From theory, there is an element x of order 8 modulo p. Hence

$p \mid (x^8 - 1)$, that is, $p \mid (x^4 - 1)(x^4 + 1)$ and either $p \mid (x^4 - 1)$ or $p \mid (x^4 + 1)$. Since x has order 8, we cannot have $p \mid (x^4 - 1)$. Hence $p \mid (x^4 + 1)$ which means that

$$x^4 \equiv -1 \pmod{p}.$$

Conversely suppose there is a solution of $x^4 \equiv -1 \pmod{p}$. We note that $(x, p) = 1$. Now

$$x^8 \equiv 1 \pmod{p}$$

so $8 \mid \phi(p) = p - 1$ i.e. $p = 8k + 1$ for some $k \in \mathbb{Z}$.

8. Suppose that $p_1, p_2, \cdots, p_n$ are the only primes of the form $8k + 1$. Let

$$Q = (p_1 p_2 \cdots p_n)^4 + 1.$$

$$\begin{aligned} \text{Since} \qquad & (8k_1 + 1)(8k_2 + 1) = 64k_1k_2 + 8k_1 + 8k_2 + 1 \\ = \quad & 8[8k_1k_2 + k_1 + k_2] + 1 \end{aligned}$$

we see that $p_1 p_2 \cdots p_n$ is of the form $8m + 1$ and hence $(p_1 p_2 \cdots p_n)^4$ is also of the form $8m + 1$. Hence Q is of the form $Q = 8m + 1 + 1 = 2(4m + 1)$.

Since $4m + 1$ is odd, we see that Q must have an odd prime factor p. Since $p_i \nmid Q$ it follows that p cannot be any of $p_1, p_2, \cdots, p_n$. Now $p \mid Q$ implies that

$$(p_1 p_2 \cdots p_n)^4 \equiv -1 \pmod{p}.$$

By Problem 7, p must be of the form $8k + 1$. This contradicts the assumption that there are only finitely many primes of the form $8k + 1$. We conclude that there are infinitely many primes of the form $8k + 1$. □

NUMBER THEORY SOLUTIONS
TUTORIAL PROBLEMS SET 5.

1. (a)

$$\begin{aligned}1^2 &\equiv 1 \pmod{3}\\ 2^2 &\equiv 1 \pmod{3}\end{aligned}$$

Hence 1 is the only quadratic residue of 3.

(b)

$$\begin{aligned}1^2 &\equiv 4^2 \equiv 1 \pmod{5}\\ 2^2 &\equiv 3^2 \equiv 4 \pmod{5}\end{aligned}$$

Hence 1 and 4 are the only quadratic residues of 5.

(c)

$$\begin{aligned}1^2 &\equiv 12^2 \equiv 1 \pmod{13}\\ 2^2 &\equiv 11^2 \equiv 4 \pmod{13}\\ 3^2 &\equiv 10^2 \equiv 9 \pmod{13}\\ 4^2 &\equiv 9^2 \equiv 3 \pmod{13}\\ 5^2 &\equiv 8^2 \equiv 12 \pmod{13}\\ 6^2 &\equiv 7^2 \equiv 10 \pmod{13}\end{aligned}$$

Hence 1, 3, 4, 9, 10, 12 are the quadratic residues of 13.

(d)

$$\begin{aligned}1^2 &\equiv 18^2 \equiv 1 \pmod{19}\\ 2^2 &\equiv 17^2 \equiv 4 \pmod{19}\\ 3^2 &\equiv 16^2 \equiv 9 \pmod{19}\\ 4^2 &\equiv 15^2 \equiv 16 \pmod{19}\\ 5^2 &\equiv 14^2 \equiv 6 \pmod{19}\\ 6^2 &\equiv 13^2 \equiv 17 \pmod{19}\\ 7^2 &\equiv 12^2 \equiv 11 \pmod{19}\\ 8^2 &\equiv 11^2 \equiv 7 \pmod{19}\\ 9^2 &\equiv 10^2 \equiv 5 \pmod{19}\end{aligned}$$

Hence 1, 4, 5, 6, 7, 9, 11, 16, 17 are the quadratic residues of 19.

2. Using Eulers' Criterion we get

$$\begin{aligned}\left(\frac{7}{11}\right) &\equiv 7^{\frac{11-1}{2}} = 7^5 \pmod{11}\\ &= 7\cdot 49\cdot 49\\ &\equiv 7\cdot 5\cdot 5 = 7\cdot 25 \pmod{11}\\ &\equiv 7\cdot 3 \pmod{11}\\ &\equiv -1 \pmod{11}\end{aligned}$$

Hence $\left(\frac{7}{11}\right) = -1$.

However it is better to use quadratic reciprocity for evaluating these symbols, as follows.

Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\begin{aligned}\left(\frac{7}{11}\right) &= -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2^2}{7}\right)\\ &= -1.\end{aligned}$$

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

If $p \equiv 1 \pmod 8$ then $p \equiv 1 \pmod 4$ and $\left(\frac{-2}{p}\right) = (1)(1) = 1$.

If $p \equiv 3 \pmod 8$ then $p \equiv 3 \pmod 4$ and $\left(\frac{-2}{p}\right) = (-1)(-1) = 1$.

If $p \equiv -1 \pmod 8$ then $p \equiv 3 \pmod 4$ and $\left(\frac{-2}{p}\right) = (-1)(1) = -1$.

If $p \equiv -3 \pmod 8$ then $p \equiv 1 \pmod 4$ and $\left(\frac{-2}{p}\right) = (1)(-1) = -1$.

4.

$$\begin{aligned}1^2 &\equiv 14^2 \equiv 1 \pmod{15}\\ 2^2 &\equiv 13^2 \equiv 4 \pmod{15}\\ 3^2 &\equiv 12^2 \equiv 9 \pmod{15}\\ 4^2 &\equiv 11^2 \equiv 1 \pmod{15}\\ 5^2 &\equiv 10^2 \equiv 10 \pmod{15}\\ 6^2 &\equiv 9^2 \equiv 6 \pmod{15}\\ 7^2 &\equiv 8^2 \equiv 4 \pmod{15}\end{aligned}$$

The solutions are $x \equiv 1, 4, 11, 14 \pmod{15}$.

5. (a) Since $3 \equiv 3 \pmod 4$ and $53 \equiv 1 \pmod 4$, using quadratic reciprocity we get,

$$\left(\frac{3}{53}\right) = \left(\frac{53}{3}\right) = \left(\frac{2}{3}\right) = -1$$

(b) Since $7 \equiv 3 \pmod 4$ and $79 \equiv 3 \pmod 4$,

$$\left(\frac{7}{79}\right) = -\left(\frac{79}{7}\right) = -\left(\frac{2}{7}\right) = -1$$

since $7 \equiv -1 \pmod 8$.

(c) $15 = 3 \cdot 5$ so

$$\left(\frac{15}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{5}{101}\right).$$

Now $\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right)$ and $\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right)$ since $101 \equiv 1 \pmod 4$. Hence

$$\begin{aligned}\left(\frac{15}{101}\right) &= \left(\frac{101}{3}\right)\left(\frac{101}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = \left(\frac{2}{3}\right) \\ &= -1.\end{aligned}$$

6. Let $n > 5$ be a positive integer and let $Q = 5(n!)^2 - 1$. Consider the prime factors of Q.

If $p \leq n$ then $p \mid 5(n!)^2$ and it follows that $p \nmid Q$. Hence all the prime factors of Q are greater than n.

Suppose $p \mid Q$. Then

$$\begin{aligned} 5(n!)^2 &= 1 + kp \quad (k \in N), \\ &\equiv 1 \qquad (\text{mod p}). \end{aligned}$$

Now $(n!, p) = 1$ so $n!$ has an inverse u modulo p. Multiplying the last congruence by u^2 we get

$$5 \equiv u^2 \quad (\text{mod p}).$$

Hence the congruence $x^2 \equiv 5$ (mod p) has a solution and this means that $\left(\frac{5}{p}\right) = 1$. Hence $\left(\frac{p}{5}\right) = 1$ by the law of quadratic reciprocity and using $5 \equiv 1 \pmod 4$. Hence the congruence $x^2 \equiv p \pmod 5$ has a solution and since the quadratic residues of 5 are 1 and 4 we conclude that either $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$.

Next we show that all the prime factors cannot be of the form $p \equiv 1 \pmod 5$. This follows easily from the fact that if $p_i \equiv 1 \pmod 4$ for $i = 1, \cdots, s$ then $p_1 p_2 \cdots p_s \equiv 1 \pmod 5$, and Q itself would have to be of the form $Q \equiv 1$ (mod 5) which is false.

This given n, there is a prime of the form $p = 5k + 4$ which divides Q and is therefore greater than n. It follows that there are infinitely many primes of the form $5k + 4$.

7. (a)

$$\begin{aligned}\left(\frac{5}{21}\right) = \left(\frac{5}{3 \cdot 7}\right) &= \left(\frac{5}{3}\right)\left(\frac{5}{7}\right) \\ = \left(\frac{2}{3}\right)\left(\frac{7}{5}\right) &= \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.\end{aligned}$$

(b) Since 101 is prime, the Jacobi symbol $\left(\frac{27}{101}\right)$ coincides with the Legendre symbol.

$$\begin{aligned}\left(\frac{27}{101}\right) &= \left(\frac{3^3}{101}\right) = \left(\frac{3}{101}\right)^3 = \left(\frac{3}{101}\right) \\ &= \left(\frac{101}{3}\right) \qquad \text{since } 101 \equiv 1 \pmod 4 \\ &= \left(\frac{2}{3}\right) = -1.\end{aligned}$$

8. $\left(\frac{30}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{3}{n}\right)\left(\frac{5}{n}\right)$

Hence $\left(\frac{30}{n}\right) = 1$ iff one of the three terms on the RHS is 1 and the other two are either both positive or both negative.

$$\begin{aligned}\left(\frac{2}{n}\right) &= (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod 8 \\ -1 & \text{if } n \equiv \pm 3 \pmod 8 \end{cases} \\ \left(\frac{5}{n}\right) &= \left(\frac{n}{5}\right) \quad \text{since} \quad 5 \equiv 1 \pmod 4 \\ \text{and} \quad \left(\frac{3}{n}\right) &= \begin{cases} \left(\frac{n}{3}\right) & \text{if } n \equiv 1 \pmod 4 \\ -\left(\frac{n}{3}\right) & \text{if } n \equiv 3 \pmod 4. \end{cases}\end{aligned}$$

Modulo 3, the quadratic residues are 1.

Modulo 5, the quadratic residues are 1, 4.

The solutions will be determined modulo $120 = 8 \cdot 3 \cdot 5$.

Case I $n \equiv 1 \pmod 8$. The solutions lie among 1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89, 97, 105, 113.

$$\left(\frac{2}{n}\right) = 1, \left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) \quad \left(\frac{5}{n}\right) = \left(\frac{n}{5}\right).$$

These conditions are satisfied when either $n \equiv 1 \pmod 3$ and $n \equiv 1, 4$ (mod 5), or $n \equiv 2 \pmod 3$ and $n = 2, 3 \pmod 5$.

Checking in the above list we find the solutions

Condition	**Solution**
$n \equiv 1 \pmod 8$, $n \equiv 1 \pmod 3$, $n \equiv 1 \pmod 5$	1
$n \equiv 1 \pmod 8$, $n \equiv 1 \pmod 3$, $n \equiv 4 \pmod 5$	49
$n \equiv 1 \pmod 8$, $n \equiv 2 \pmod 3$, $n \equiv 2 \pmod 5$	17
$n \equiv 1 \pmod 8$, $n \equiv 2 \pmod 3$, $n \equiv 3 \pmod 5$	113

Note that to get each solution we have to solve a system of linear congruences which could also be done using the Chinese Remainder Theorem.

Case II $n \equiv (-1) \pmod 8$. In this case $\left(\dfrac{3}{n}\right) = -\left(\frac{n}{3}\right)$

As above we get another 4 solutions

$$71, 119, 7, 103$$

Case III $n \equiv 3 \pmod 8$. In this case $\left(\dfrac{3}{n}\right) = -\left(\frac{n}{3}\right)$ and $\left(\dfrac{2}{n}\right) = -1$ and we get the solutions

$$19, 91, 107, 83$$

Case IV $n \equiv -3 \pmod 8$. Then $\left(\dfrac{2}{n}\right) = -1$ and $\left(\dfrac{3}{n}\right) = \left(\frac{n}{3}\right)$ and we get the solutions

$$37, 13, 101, 29.$$

NUMBER THEORY SOLUTIONS
TUTORIAL PROBLEMS SET 6.

1. (a) Let

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m > n,\ (m, n) = 1$, and one of $m,\ n$ is odd, the other even. For $z \leq 40$ we must have $m^2 < 40$ so $m \leq 6$. The solutions are listed below.

m	n	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37

(b) We get all other Pythagorean triples by taking integral multiples of primitive triples. For $z \leq 40$ the additional triples are:

x	y	z
6	8	10
9	12	15
12	16	20
15	20	25
18	24	30
21	28	35
24	32	40
10	24	26
15	36	39
30	16	34

2. Suppose that $n > 2$ and that both

$$\begin{aligned} x^2 + y^2 &= z^2 \\ \text{and} \quad x^n + y^n &= z^n. \end{aligned}$$

Note that $x < z$ and $y < z$ since $x \neq 0,\ y \neq 0$. Then

$$\begin{aligned} x^n + y^n &= x^2 x^{n-2} + y^2 y^{n-2} \\ &< x^2 z^{n-2} + y^2 z^{n-2} \\ &= (x^2 + y^2) z^{n-2} \\ &= z^2 z^{n-2} = z^n \end{aligned}$$

This is a contradiction so we cannot have both $x^2+y^2=z^2$ and $x^n+y^n=z^n$.

3. From $m=a^2+b^2$ and $n=c^2+d^2$ we get

$$mn=a^2c^2+a^2d^2+b^2c^2+b^2d^2=(ac+bd)^2+(ad-bc)^2.$$

4. The equation can be rewritten as $(x+y)^2=x^2y^2+xy$. Substitute $x+y=a$ and $xy=b$ (If x,y are integers then so are a,b). Then $a^2=b^2+b=b(b+1)$. Now substitute $b=c+\frac{1}{2}$. Then $a^2=(c+\frac{1}{2})(c-\frac{1}{2})$. It follows

$$c^2-a^2=(c-a)(c+a)=\frac{1}{4}.$$

Now $c-a=\frac{\alpha}{2}$ and $c+a=\frac{\beta}{2}$ where α,β are integers. The equation above is only possible if α and β are both equal to ±1. Then $a=0$ and $c=\pm\frac{1}{2}$. Hence $b=0$ or $b=1$. Then $x=-y$ and x is either 0 or ±1. The solutions are $\{(0,0),(1,-1),(-1,1)\}$.