Show all your work. Justify your solutions. Answers without justification will not receive full marks.

Only hand in the problems on page 2.

Practice Problems

Question 1. Prove that if $a \mid b$ and $a \mid 3c$ then $a \mid 6(a+b+c)$.

Solution: We have $a \mid b$ and $a \mid 3c$, so by definition $b = ma$ and $3c = na$, where $m, n \in \mathbb{Z}$. Therefore

$$6(a+b+c) = 6a + 6b + 2(3c) = 6a + 6ma + 2na = a(6 + 6m + 2n).$$

Hence $a \mid 6(a+b+c)$. □

Question 2. Find integers x and y that solve each of the following equations, or explain why no solution exists.

(a) $30x + 26y = 2$.
(b) $30x + 26y = 16$.
(c) $60x + 42y = 8$.
(d) $927979x + 823543y = 1$

Solution:

(a)

	30	1	0
1	26	0	1
6	4	1	−1
2	$\boxed{2}$	−6	7

$\gcd(30, 26) = 2$ and $2 \mid 2$, therefore a solution exists, namely

$$30 \cdot (-6) + 26 \cdot 7 = 2$$

ie $x = -6$, $y = 7$.

(b) $\gcd(30, 26) = 2 \mid 16$, so a solution exists. Multiplying the equation above by 8 gives

$$30 \cdot (-48) + 26 \cdot 56 = 16$$

ie $x = -48$, $y = 56$.

(c)

	60
1	42
2	18
3	$\boxed{6}$
	0

Thus $\gcd(60, 42) = 6$. There is no solution since $6 \nmid 8$ (so we don't need the extra columns).

(d)

	927979	1	0
1	823543	0	1
7	104436	1	-1
1	92491	-7	8
7	11945	8	-9
1	8876	-63	71
2	3069	71	-80
1	2738	-205	231
8	331	276	-311
3	90	-2413	2719
1	61	7515	-8468
2	29	-9928	11187
9	3	27371	-30842
1	2	-256267	288765
	$\boxed{1}$	283638	-319607

So $\gcd(927979, 823543) = 1$, and

$$927979 \cdot 283638 + 823543 \cdot -319607 = 1.$$

Question 3. Without using the Fundamental Theorem prove the following: If $\gcd(a, b) = \gcd(a, c) = 1$ and $a \mid bcd$, then $a \mid d$.

Solution: Since $\gcd(a, b) = 1$ and $a \mid bcd = b(cd)$, then $a \mid cd$ (by Theorem 1.7.1). Since $\gcd(a, c) = 1$ and $a \mid cd$, then $a \mid d$ (again by Theorem 1.7.1).

Question 4. Let $\gcd(w, x, y, z)$ be the largest integer dividing all of w, x, y, z.

(a) Prove that $\gcd(\gcd(w, x), \gcd(y, z)) = \gcd(w, x, y, z)$.
(b) Hence find $\gcd(252, 112, 147, 98)$.

Solution:

(a) Let $a = \gcd(w, x)$, $b = \gcd(y, z)$, $c = \gcd(a, b)$, and $d = \gcd(w, x, y, z)$. We need to show that $c = d$.

First prove $c \leq d$: By definition of gcd, we have $a \mid w$, $a \mid x$, $b \mid y$, $b \mid z$, $c \mid a$ and $c \mid b$. Since $c \mid a$ and $a \mid w$, then $c \mid w$. In a similar way $c \mid x$ (since $c \mid a$ and $a \mid x$), $c \mid y$ (since $c \mid b$ and $b \mid y$), and $c \mid z$ (since $c \mid b$ and $b \mid z$). Therefore $c \leq \gcd(w, x, y, z) = d$.

Now prove $d \leq c$: By definition $d = \gcd(w, x, y, z)$, so $d \mid w$, $d \mid x$, $d \mid y$, and $d \mid z$. Since $d \mid w$ and $d \mid x$, $d \mid \gcd(w, x) = a$. Since $d \mid y$ and $d \mid z$, $d \mid \gcd(y, z) = b$. Thus $d \leq \gcd(a, b) = c$. □

(b)

	252		147		49
2	112	1	98	1	28
4	$\boxed{28}$	2	$\boxed{49}$	1	21
	0		0	3	$\boxed{7}$
					0

We have $\gcd(252, 112) = 28$, $\gcd(147, 98) = 49$, and $\gcd(49, 28) = 7$.
Thus by (a), $\gcd(252, 112, 147, 98) = 7$.

Question 5. Calculate the last decimal digit of $(1997^{1997})^{1997}$.

Solution: The last decimal digit can be found by finding $1997^{1997} \pmod{10}$.

$1997^1 \equiv 7,\ 1997^2 \equiv 7^2 \equiv 9,\ 1997^3 \equiv 9 \cdot 7 \equiv 3,\ 1997^4 \equiv 3 \cdot 7 \equiv 1 \pmod{10}$.

We use $1997^4 \equiv 1$ to simplify the expression. Since $1997 = 4 \cdot 499 + 1$, we have

$$1997^{1997} = 1997^{4 \cdot 499 + 1} = (1997^4)^{499} \cdot 1997^1 \equiv 1^{499} \cdot 7 \equiv 7.$$

Thus $(1997^{1997})^{1997} \equiv 7^{1997} \pmod{10}$. But we have already shown that $7^{1997} \equiv 1997^{1997} \equiv 7 \pmod{10}$. Therefore $(1997^{1997})^{1997} \equiv 7 \pmod{10}$, so the last decimal digit is 7.

Question 6. Prove that for all $a \in \mathbb{Z}$, $8 \mid [a^2 + (a-2)^2 - 2]$ or $8 \mid [a^2 + (a-2)^2 - 4]$.

Solution: We need to show that $a^2 + (a-2)^2 \equiv 2, 4 \pmod{8}$. We consider the 8 congruence classes (mod 8). All answers are taken mod 8.

a	0	1	2	3	4	5	6	7
a^2	0	1	4	1	0	1	4	1
$(a-2)^2$	4	1	0	1	4	1	0	1
$a^2 + (a-2)^2$	4	2	4	2	4	2	4	2

In each case $a^2 + (a-2)^2 \equiv 2, 4 \pmod{8}$. □

Assignment Problems

Question 1. For each of the equations below, either find a solution in integers x, y, or prove that no solution exists.

(a) $30x + 21y = 3$.
(b) $30x + 21y = 15$.
(c) $30x + 21y = 10$.
(d) $41x + 42y = 2010$.

Solution: The initial set up is:

i	q_i	r_i	x_i	y_i
-1	—	30	1	0
0	?	21	0	1

We have $30/21 \simeq 1.43$ so $q_0 = 1$. Using Euclid's algorithm we get:

i	q_i	r_i	x_i	y_i
-1	—	30	1	0
0	1	21	0	1
1	2	9	1	-1
2	3	3	-2	3
		0		

Hence:

(a) $\gcd(30, 21) = 3$ and $30 \cdot (-2) + 21(3) = 3$.

(b) Multiplying by 5, $30 \cdot (-10) + 21(15) = 15$.

(c) $\gcd(30, 21) = 3 \nmid 10$ so the equation is not solvable.

(d) Euclid gives $41 \cdot (-1) + 42 \cdot 1 = 1$, so $41 \cdot (-2010) + 42(2010) = 2010$ (obviously!)

Question 2. Calculate $d = \gcd(1234567890,\ 987654321)$, and find integers x and y with $1234567890\,x + 987654321\,y = d$.

Solution: The initial set up is:

i	q_i	r_i	x_i	y_i
-1	—	1234567890	1	0
0	?	987654321	0	1

We have $r_{-1}/r_0 \simeq 1.25$, so we round down to obtain $q_0 = 1$. There is no need to write down the column for the counter i. We obtain:

q_i	r_i	x_i	y_i
—	1234567890	1	0
1	987654321	0	1
4	246913569	1	-1
5486968	45	-4	5
5	9	21947873	-27434841
	0		

Thus the gcd is 9, and $1234567890 \cdot (21947873) + 987654321 \cdot (-27434841) = 9$.

Compare this approach to factorizing: $1234567890 = 2 \cdot 3^2 \cdot 5 \cdot 3607 \cdot 3803$, and $987654321 = 3^2 \cdot 17^2 \cdot 379721$. After removing the obvious factors, we would have to factor $13717421 = 3607 \cdot 3803$, and show that 379721 is prime to be certain the gcd is 9.

Also there is no need to do find the gcd and then work by back substituting to get the gcd as a linear combination; it all works out simultaneously with Euclid's algorithm.

Question 3.

(a) Define $F_0 = 1$, $F_1 = 1$ and recursively define $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. These are the *Fibonacci* numbers. Calculate F_{10} and F_{11}.
(b) Calculate $d = \gcd(F_{10}, F_{11})$, and write d as a linear combination of F_{10} and F_{11}. What do you notice?
(c) Prove that $\gcd(F_{n+1}, F_n) = 1$ for all $n \geq 0$.

Solution:

(a) $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, $F_3 = 3$, $F_4 = 5$, $F_5 = 8$, $F_6 = 13$, $F_7 = 21$, $F_8 = 34$, $F_9 = 55$, $F_{10} = 89$, $F_{11} = 144$.

(b)

q_i	r_i	x_i	y_i
—	144	1	0
1	89	0	1
1	55	1	−1
1	34	−1	2
1	21	2	−3
1	13	−3	5
1	8	5	−8
1	5	−8	13
1	3	13	−21
1	2	−21	34
1	1	34	−55
	0		

So $\gcd(F_{11}, F_{10}) = 1$ and $F_{11} \cdot 34 - F_{10} \cdot 55 = 1$. The required coefficients are also Fibonacci numbers. Also, all quotients obtained are 1, and the remainders are all Fibonacci numbers.

Indeed, since $F_n = 1 \cdot F_{n-1} + F_{n-2}$, starting from F_n and F_{n-1}, the next remainder will be F_{n-2} and so on. Thus all the quotients are 1, and the remainders are the successive Fibonacci numbers. Similarly, the x and y columns are Fibonacci numbers, with alternating signs in front. So we can conjecture that $\begin{vmatrix} F_n & F_{n-1} \\ F_{n-2} & F_{n-3} \end{vmatrix} = (-1)^{n-1}$. This can be easily proved by induction. Note that it implies $\gcd(F_n, F_{n-1}) = 1$.

It requires n lines of calculation to calculate $\gcd(F_n, F_{n-1})$. This is the worst scenario for Euclid's algorithm, because in each step the quotient is always be 1, so the remainders decrease as slowly as possible. In other words, if a, $b \leq F_n$ then the calculation of $\gcd(a, b)$ will take at most n lines.

Fact: $F_n \simeq 1.618^n$. So if $b < a \approx F_n \approx 1.618^n$ then $n \approx \log a / \log(1.618) \approx 2.1 \log a$. So the number of steps needed will be $\lessapprox 2 \log a$, even in the worst case.

(c) Clearly $\gcd(F_1, F_0) = 1$. Now inductively assume $\gcd(F_n, F_{n-1}) = 1$ for $n \leq k$. Then $\gcd(F_{k+1}, F_k) = \gcd(1 \cdot F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1})$ by theorem 1.5.1, and this is 1 by inductive hypothesis.

Question 4.

(a) Prove that if $d \mid a$ and $d \mid b$ then $d \mid (ax + by)$ for any integers x and y.

(b) Prove that last decimal digit of any perfect square must be 0, 1, 4, 5, 6 or 9. Hint: compare example 1.4.4.
(c) Prove that for any integer a the number $a(a^2-7)$ is a multiple of 6.

Solution:

(a) If $d \mid a$ then $a = de$ for some integer e. If $d \mid b$ then $b = df$ for some integer f. Thus $ax + by = dex + dfy = d(ex + fy)$, so $d \mid (ax + by)$, by definition.

(b) By the division algorithm, we can write any integer in the form $n = 10m + r$ with $r \in \{0, 1, \ldots, 9\}$. Thus $n^2 = (10m + r)^2 = 100m^2 + 20mr + r^2 = 10(10m^2 + 2mr) + r^2$. Therefore, the last digit of n^2 is the same as the last digit of r^2. But 0^2 ends in 0, 1^2 in 1, 2^2 in 4 etc, and 9^2 ends in 1, so only 0, 1, 4, 5 and 9 are possible.

This proof is much neater when written using modular arithmetic. We have $n \equiv r \pmod{10}$ for $r \in \{0, 1, \ldots, 9\}$, and we check that $0^2 \equiv 0$, $1^2 \equiv 1$, $\ldots$, $9^2 \equiv 1 \pmod{10}$. We could shorten this even more by letting $r \in \{-4, -3, \ldots, 4, 5\}$, since $(\pm 4)^2 \equiv 6 \pmod{10}$ etc.

(c) We work mod 6.

a	0	1	2	3	4	5
a^2	0	1	4	3	4	1
a^2-7	5	0	3	2	3	0
$a(a^2-7)$	0	0	0	0	0	0

In every case $a(a^2 - 7) \equiv 0 \pmod{6}$.

Question 5.

(a) Prove that $\sqrt{3}$ is irrational.
(b) Prove that $\sqrt[3]{2}$ is irrational.
(c) Prove that the equation $x^5 - 3y^5 = 2008$ has no solution in integers x, y. Hint: mod 11.

Solution:

(a) Suppose $\sqrt{3} = m/n$ with m, $n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Then $3n^2 = m^2$. Clearly 3 divides the LHS so $3 \mid m^2 = m \cdot m$. But 3 is prime, so by Euclid's result $3 \mid m$ (since Euclid tells us that $3 \mid m$ or $3 \mid m$). Let $m = 3k$ and substitute back: $3n^2 = m^2 = (3k)^2 = 9k^2$, so $n^2 = 3k^2$. Now by the same argument $3 \mid n$ so $\gcd(m, n) \geq 3$, a contradiction.

A shorter proof, assuming the fundamental theorem: consider the power of 3 occurring in the unique factorization of the LHS and the RHS. If $n = 3^a P$ where P is a product of other primes (not 3's) then the power of 3 occurring on the LHS is odd. But the power of 3 in the RHS is even. Contradiction.

(b) Suppose $\sqrt[3]{2} = m/n$ with m, $n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Then $2n^3 = m^3$. Clearly 2 divides the LHS so $2 \mid m^3$. But 2 is prime, so by Euclid's result $2 \mid m$ (applying Euclid's result to products of length 3). Let $m = 2k$ and substitute back: $2n^3 = m^3 = (2k)^3 = 8k^3$, so $n^3 = 4k^2$. Now 2 divides the RHS so $2 \mid n^3$ and by the same argument $2 \mid n$ so $\gcd(m, n) \geq 2$, a contradiction.

(c) Check that $x^3 \equiv 0$ or $\pm 1 \pmod{11}$ for $x = 0, 1, \ldots, 10$. The LHS is $\{0, \pm 1\} - 3\{0, \pm 1\}$, so the possibilities for the LHS are $\{0, 1, 2, 3, 4, 7, 8, 9, 10\} \pmod{11}$, but $2008 \equiv 6 \pmod{11}$.

Question 6. I have an unlimited stock of 4 cent and 7 cent stamps. Which postages can I make? Which postages can I not make? Prove your answer. Note: negative numbers of stamps cannot be used. In other words, which $n \in \mathbb{N}$ can be written in the form $n = 4x + 7y$ with x, $y \geq 0$?

Solution: Since $\gcd(4,7)=1$, the equation $4x+7y=n$ has a solution in integers x and y for any n. However some of these solutions involve negative x or y. Eg $4\cdot(-2)+7\cdot(1)=1$. This is not allowed.

Let $P=\{4x+7y \mid x,y\in\mathbb{Z}, x,y\geq 0\}$. Let's experiment by picking values for x, $y\geq 0$ and seeing which n occur (sorting according to increasing n):

x	0	1	0	2	1	3	0	2	4	1	3	5	0
y	0	0	1	0	1	0	2	1	0	2	1	0	3
$n=4x+7y$	0	4	7	8	11	12	14	15	16	18	19	20	21

If (x,y) is not listed: if $y=0$ then $x\geq 6$ so $n>20$, if $y=1$ then $x\geq 4$ and $n>20$, if $y=2$ then $x\geq 2$ and $n>20$. So all $n\in P$ with $n\leq 20$ are listed.

We see that 18, 19, 20 and $21\in P$. But by adding another 4 cent stamp to each of these, 22, 23, 24 and $25\in P$. Adding one more 4 cent stamp, 26, 27, 28, $29\in P$ etc.

More formally, if $n\in P$ and $m\in P$ with $m\equiv n \pmod 4$ and $m\geq n$ then $m=n+4k$ for some $k\geq 0$ and so $m\in P$. Let $n\geq 18$. If $n\equiv 0 \pmod 4$ then $n\equiv 20 \pmod 4$ with $20\in P$, so $n\in P$. If $n\equiv 1 \pmod 4$ then $n\equiv 21 \pmod 4$ with $21\in P$, so $n\in P$. Similarly if $n\equiv 2$ or $3 \pmod 4$.

Thus all $n\geq 18$ are in P, as well as the smaller amounts given in the table. That is, $P=\{0,4,7,8,11,12,14,15,16\}\cup\{n\in\mathbb{N}\mid n\geq 18\}$.

More generally if $\gcd(a,b)=1$ then every postage $\geq (a-1)(b-1)$ can be made. Wilhelm Fliess, a longtime correspondent with Sigmund Freud, believed in "biorhythm theory" according to which humans experience 23 and 28 day cycles. This idea originated because Fleiss was fascinated by the observation that many important numbers in his life could be expressed as $23x+28y$, a fact which is hardly surprising ...