Cubo Matemática Educacional
Vol. 4, Nº1, MAYO 2002

CHINESE REMAINDER THEOREM, ANCIENT AND CONTEMPORARY

Paulo Brumatti & Plamen Koshlukov
IMECC, UNICAMP, Cx. P. 6065
13083-970 Campinas, SP, Brasil
e-mails: brumatti@ime.unicamp.br;
plamen@ime.unicamp.br

1 Introduction

In this note we consider a rather elementary but important assertion, namely the Chinese Remainder Theorem. In Section 2 we give various applications, and finally, in Section 3, we provide a list of exercises for the reader.

The note is aimed at School students with proven interest in Mathematics, at their teachers, and at University students who have not lost (or forgotten) their interest to problem solving. It could be used in preparation for Math competitions and olympiads. For further reading we would like to suggest the books [2] and [3] that are readily available in Portuguese. (Note that the first of them has been translated to English as well.)

Throughout we consider integers. We suppose the reader is familiar with the notion of congruence and its basic properties.

Let a and m be integers, $m > 1$ and $(a, m) = 1$. The last notation means that the *greatest common divisor* GCD of a and m equals 1 i.e., a and m are coprime. It is well known that the congruence $ax \equiv b \pmod{m}$ has unique solution $x_0 \in [0, m-1]$, and its solutions are given by $x_t = x_0 + mt$, $t \in \mathbb{Z}$. In order to prove this fact one considers all residues modulo m, the integers $\{0, 1, \ldots, m-1\}$, and multiplies them by a. Since $(a, m) = 1$ the integers $\{0.a, 1.a, \ldots, (m-1).a\}$ are pairwise distinct modulo m and hence modulo m they represent a permutation of the first system. Therefore some of the latter numbers, say x_0, satisfies $ax_0 \equiv b \pmod{m}$. Now let us try to generalise this fact. Such generalisations were discovered by the ancient Chinese and Greek mathematicians long ago. Of course it was not asserted in the form we are going to present but in essence it was the same.

Theorem 1 (Chinese Remainder Theorem) *Let $n \geq 1$, and let m_1, m_2, $\ldots$, m_n be pairwise coprime positive integers. Suppose that a_1, a_2, $\ldots$, a_n are such that $(a_i, m_i) = 1$, $i = 1, 2, \ldots, n$, and that b_1, b_2, $\ldots$, $b_n \in \mathbb{Z}$. Then the system of congruences*

$$| \, a_i x \equiv b_i \pmod{m_i}, \qquad i = 1, 2, \ldots, n$$

has unique solution $x_0 \in [0, m-1]$ where $m = m_1 m_2 \ldots m_n$. All integer solutions of this system are given by the formula $x_t = x_0 + mt$, $t \in \mathbb{Z}$.

Proof. We give a sketch of the proof. Use an induction on n. The case $n = 1$ was dealt with the above comments. If $n = 2$, the solutions of $a_1 x \equiv b_1 \pmod{m_1}$ are $x_t = x_0 + m_1 t$. Now substitute this expression for x_t in the second congruence. One obtains $a_2(x_0 + m_1 t) \equiv b_2 \pmod{m_2}$ and $(a_2 m_1)t \equiv b_2 - a_2 x_0 \pmod{m_2}$. The last congruence admits unique solution t_0 in $[0, m_2 - 1]$. Now we leave to the reader the completion of the induction argument. (Notice that the argument above justifies both the base and the step of the induction. Why starting the induction from $n = 1$ is not sufficient?)

Now we outline another, direct proof of the Chinese Remainder theorem. Denote by $M_i = \prod_{j \neq i} m_j$, $i = 1, 2, \ldots, n$. Observe that M_i and m_i are coprime (Why?). Therefore the congruence $M_i y \equiv 1 \pmod{m_i}$ admits a solution, say N_i. Denote further c_i a solution of the congruence $a_i x \equiv b_i \pmod{m_i}$. Since m_j divides M_i for $j \neq i$ then

$$a_i \sum_{j=1}^{n} M_j N_j c_j \equiv a_i M_i N_i c_i \equiv a_i c_i \equiv b_i \pmod{m_i}$$

for every i, and we can take $x_0 = \sum_{j=1}^{n} M_j N_j c_j$ as a solution of the system.

In fact both proofs of the theorem give us an algorithm for solving linear systems of congruences. If the numbers m_i are not coprime the same methods yield the solutions (or show that the system is incompatible).

Now let us make some very brief historical comments. The Chinese Remainder theorem (as its name shows) dates back to the third century' China Mathematics. Approximately at the same time Greek scientists used a similar algorithm in resolving practical questions. Much later, in 19th century, the theorem was generalised to large extent. But explaining to what extent would leave us outside the scope of the present note.

Essentially the Chinese Remainder theorem is an elementary fact. Surprisingly enough, it has various applications, and some of them are quite interesting and difficult, as we shall try to convince the reader.

2 Applications

A well known exercise asks whether for every n there exist n consecutive composite integers. One gives an example: $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$. In this sequence, the i-th term is divisible by $i+1$, and it is obviously larger than i. Now we consider some variations of this fact, of course applying the Chinese remainder theorem. Note that such constructions sometimes are quite difficult to find, and could be rather tricky to invent. Fortunately the Chinese Remainder Theorem provides some "canonical" approach to such questions. The above example can be resolved easily by observing that the system $x + k \equiv 0 \pmod{p_k}$ has solutions, and its solutions form an arithmetic progression. Here p_k stands for the k-th prime, thus $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc.

Exercise 1 *Let $a + bm$, $m = 1, 2, \ldots$, be an infinite arithmetic progression where $a, b \in \mathbb{N}$. Prove that for every n there exist n consecutive elements of the progression that are composite.*

Solution. The solution is a slight modification of the above reasoning. Choose primes $b < r_1 < r_2 < \cdots < r_n$, and consider the congruences $a + bx \equiv -ib \pmod{r_i^2}$, $i = 1, 2, \ldots, n$. These congruences have solution $x \in \mathbb{N}$ and $a + b(x + i) \equiv 0 \pmod{r_i^2}$ for every i. Therefore the n consecutive terms of $a + bm$ namely $\{a + b(x + i) \mid i = 1, 2, \ldots, n\}$ are composite.

Exercise 2 *Prove that:*

a) There does not exist an infinite arithmetic progression all of whose terms being exponents of positive integers;

b) For every n there exist n-term arithmetic progressions consisting of exponents of positive integers;

c) For every n there exist n consecutive positive integers none of which is an exponent.

(Here by exponent we mean non-trivial exponent i.e. positive integers of the form a^k, $k > 1$.)

Solution. a) Let $a + mb$, $m = 0, 1, 2, \ldots$, be an infinite arithmetic progression, and choose a prime $p > a + b$. Then $(b, p) = (b, p^2) = 1$, and there exist integers x and y with $xb - yp^2 = 1$ (Why?). Put $m = x(p - a)$, then $a + mb = p + (yp - ya)p^2$ is divisible by p but not by p^2. Obviously $a + mb$ belongs to our arithmetic progression but it cannot be an exponent.

b) Denote by p_i the i-th prime. Set $p = p_1 p_2 \ldots p_m$, and let $q_i = p \mid p_i$, $i = 1, 2, \ldots, m$. Now consider the system of two congruences $x \equiv 0 \pmod{q_i}$, $x \equiv -1$

(mod p_i). Since $(p_i, q_i) = 1$ this system has solution, denote it as x_i. Now denote $d = 1^{x_1}2^{x_2}\dots m^{x_m}$. We shall show that the progression $\{d, 2d, 3d, \dots, md\}$ consists of exponents. According to the choice of x_i we have that $p_i \mid x_j$ if $j \neq i$ and that $p_i \mid (x_i + 1)$ for every i. Hence

$$d_n = nd = \left(n^{(x_n+1)/p_n} \prod_{i \neq n} i^{x_i/p_n} \right)^{p_n}$$

are exponents.

c) If p_i is the i-th prime the system

$$| \, x \equiv p_i - i + 1 \pmod{p_i^2}, \qquad i = 1, 2, \dots, n,$$

has positive integer solution r. Then the integers $r + i - 1$, $i = 1, 2, \dots, m$, give the desired example.

An intriguing and rather complicated problem that has been attracting the attention of lots of mathematicians is the following. Does there exist a function whose values are exactly the primes? We already know that if exists, such function cannot be linear. On the other hand, a famous theorem due to P. L. Dirichlet states that in every arithmetic progression $a + nb$, $n = 1, 2, \dots$, with $(a, b) = 1$ there exist infinitely many primes. The proof of this theorem is complicated and there seem to be no elementary proofs of it. The interested reader can get an idea on how this theorem is proved in [1], Chapter 7, or in [7], Chapters 12, 13. We provide several particular cases of it in the last section. (But do not cheat and do not use Dirichlet's theorem for these exercises...)

Let us return to functions that "generate" the primes. In 1971 Yuri Matiyasevich found a polynomial with integer coefficients with the following property. For every positive integer values of its 24 variables the values of this polynomial are positive primes, and every positive prime can be obtained in this way, as a value of this polynomial. The polynomial discovered by Matiyasevich is of degree 37. Notice that this result is by no means elementary; it is consequence of the solution of the Tenth Hilbert problem that concerns solvability of Diophantine equations. We refer to Matiyasevich' book [5] for details. (A warning: the book is rather difficult and requires a lot of advanced knowledge.) Let us recall that a Diophantine equation is an equation that has to be solved in integers (or, sometimes, in rational numbers). A typical example is the equation $x^n + y^n = z^n$ where $n \geq 2$ is given, and the (integer) variables are x, y, z. When $n = 2$ its solutions are the Pythagorean triples, i.e. they describe the right triangles whose sides are integers. When $n > 2$ it was conjectured, centuries ago, by P. Fermat that this equation does not have solutions in positive integers. This problem became famous as the "Fermat's last theorem", it was recently resolved by A. Wiles. The proof of Fermat's theorem was one of the greatest achievements of the Mathematics of the 20th century. We do not give reference for this important result since it is indeed extremely complicated; on the other hand, Wiles' achievement was discussed, even in "popular" texts.

Now we show that functions generating the primes cannot be polynomials in one variable either. But first let us make the following observation. Let $f(x)$ be a polynomial with integer coefficients and let a, $b \in \mathbb{Z}$ be such that $a \equiv b \pmod{m}$, $m \in \mathbb{N}$. Then $f(a) \equiv f(b) \pmod{m}$. For the proof notice that m divides $a^k - b^k$ for every $k \geq 0$.

Exercise 3 *Let $f(x)$ be a nonconstant polynomial with integer coefficients. Then there exist infinitely many:*

a) Primes p such that the congruence $f(x) \equiv 0 \pmod{p}$ has solution;

b) Integers $x \in \mathbb{Z}$ such that $f(x)$ is composite;

c) Integers $x \in \mathbb{Z}$ such that $f(x)$ is composite and has 2000 distinct prime divisors.

Solution. a) If $f(x) = x$ then we know that there exist infinitely many primes (Euclid's Theorem). We shall simulate Euclid's proof of this fact. Suppose that the congruences $f(x) \equiv 0 \pmod{p_i}$ admit solutions where p_i are pairwise distinct primes, $i = 1, 2, \ldots, k$. (Such primes do exist since $f(x)$ is non-constant.) We shall find another prime p_{k+1} such that $f(x) \equiv 0 \pmod{p_{k+1}}$ has solution, too. Let y be variable, and write

$$f(x+y) = f(x) + g_1(x)y + g_2(x)y^2 + \cdots + g_n(x)y^n = f(x) + yA$$

where $n = \deg f$ is the degree of f, g_1, g_2, $\ldots$, g_n are polynomials with integer coefficients, and A is an integer.

Now let $x \in \mathbb{N}$ be such that $f(x) = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $e_i \geq 0$, and set $y = p_1 p_2 \ldots p_k f(x)$. Then we obtain that $f(x+y) = f(x)(1 + Ap_1p_2 \ldots p_k)$. Take a prime divisor q of $1 + Ap_1p_2 \ldots p_k$, obviously $q \notin \{p_1, p_2, \ldots, p_k\}$. Thus $p_{k+1} = q$ and we are done. (Why one may suppose that $A \neq 0$?)

b) (Hint) Apply (a) together with the Chinese Remainder Theorem.

c) (Hint) Let $f(x_1) \equiv 0 \pmod{p_1}$ and $f(x_2) \equiv 0 \pmod{p_2}$ for distinct primes p_1 and p_2. Prove that for every x such that $x \equiv x_1 \pmod{p_1}$ and $x \equiv x_2 \pmod{p_2}$ one has $f(x) \equiv 0 \pmod{p_i}$, $i = 1, 2$.

Having proved that polynomial functions (in one variable) cannot "generate" the sequence of the primes now we turn to exponential functions. We show that certain exponential functions cannot generate the primes and even that they consist of composite numbers only. We shall return to this topic in the last section.

Exercise 4 *Let $a_n = a_n(k) = k.2^n + 1$, $n = 1$, 2, $\ldots$, where $k \in \mathbb{N}$. Prove that there exist infinitely many k such that every a_n is composite.*

Solution. We shall use the following classical and well known fact. Let $F_n = 2^{2^n} + 1$ be the Fermat numbers. Then $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are primes. Leonard Euler proved that F_5 is composite, and it equals the product $F_5 = 2^{32} + 1 = 641.p$ where p is prime, $p > F_4$. (We suggest that the reader prove $F_5 \equiv 0 \pmod{641}$ using the following hint: $641 = 5^4 + 2^4 = 5.2^7 + 1$.)

Now consider the system of the congruences

$$\left|\begin{array}{lcl} x & \equiv & 1 \pmod{F_0} \\ x & \equiv & 1 \pmod{F_1} \\ x & \equiv & 1 \pmod{F_2} \\ x & \equiv & 1 \pmod{F_3} \\ x & \equiv & 1 \pmod{F_4} \\ x & \equiv & 1 \pmod{641} \\ x & \equiv & -1 \pmod{p} \end{array}\right.$$

It has infinitely many solutions x. Take a solution k of this system such that $k > p$. We shall prove that all $a_n(k)$ are composite. But first note that one can write the above system as follows.

$$\left|\begin{array}{lcl} x & \equiv & 1 \pmod{641(F_5-2)} \\ x & \equiv & -1 \pmod{p} \end{array}\right.$$

Let $n = 2^m t$ for t odd. If $0 \leq m \leq 4$ then

$$a_n(k) = k.2^n + 1 \equiv 2^{2^m t} + 1 \equiv (-1)^t + 1 \equiv 0 \pmod{F_m}$$

since F_m divides $2^{32} - 1$ for $0 \leq m \leq 4$. (Prove the last statement!) But $k > p$ implies $a_n(k) > p > F_4 \geq F_m$ hence a_n is composite.

Now assume $m = 5$. Then $a_n = k.2^n + 1 = k.2^{t.2^5} + 1 \equiv 2^{2^5}t + 1 \equiv 0 \pmod{641}$ is composite, too.

Finally if $m \geq 6$ we represent $n = 2^6 r$ where $r \geq 1$, and then $k.2^n + 1 \equiv -2^{2^6}.r + 1 \pmod{p}$. Combine this with $2^{2^6 r} - 1 = (2^{2^6} - 1).a = (2^{2^5} - 1)(2^{2^5} + 1).a \equiv 0 \pmod{p}$. Hence in this case a_n is also composite.

In order to continue we shall need some facts concerning congruences of the form $f(x) \equiv 0 \pmod{p^a}$.

Theorem 2 *Let $f(x)$ be a nonconstant polynomial with integer coefficients.*

a) Let f' be the derivative of f. If the congruence $f(x) \equiv 0 \pmod{p}$ has integer solution x_0 such that $f'(x_0) \not\equiv 0 \pmod{p}$ then the congruence $f(x) \equiv 0 \pmod{p^a}$ has solution for every $a \geq 1$.

b) If f and f' are coprime polynomials (this is the case when f is irreducible over the integers, for example) then there exist infinitely many primes p such that the congruence $f(t) \equiv 0 \pmod{p}$ implies $f'(t) \not\equiv 0 \pmod{p}$.

Proof. a) We make use of the Taylor expansion of f:

$$\begin{aligned} f(x) &= f(x_0) + (x - x_0)f'(x_0) + (x - x_0)^2 f''(x_0)/2! \\ &\quad +(x - x_0)^3 f'''(x_0)/3! + \cdots + (x - x_0)^n f^{(n)}(x_0)/n! \end{aligned}$$

where $n = \deg f$. You do not need calculus to prove the validity of this formula; a simple induction yields the result (at least in case of polynomials).

Now since $f(x_0) \equiv 0 \pmod{p}$ we know that $f(x_0 + tp) \equiv 0 \pmod{p}$ for every $t \in \mathbb{Z}$. We put in Taylor's formula $x = x_0 + tp$, and thus we obtain

$$\begin{aligned} f(x_0 + tp) &= f(x_0) + tpf'(x_0) + (tp)^2 f''(x_0)/2! + (tp)^3 f'''(x_0)/3! + (tp)^n f^{(n)}(x_0)/n! \\ &= f(x_0) + tpf'(x_0) + p^2 A \end{aligned}$$

where A is some rational number. Consider the polynomial $p(x) = x^s$, the r-th derivative of $p(x)$ equals $s!/(s-r)!x^{s-r}$ if $s \geq r$, and it is 0 otherwise. Now observe that $r!$ divides $s!/(s-r)!$ (Why?) therefore A is actually integer. Consider the congruence

$$tf'(x_0) \equiv -f(x_0)/p \pmod{p}$$

where t is the new "variable." (The right hand side fraction is an integer since $f(x_0)$ is divisible by p.) The congruence has an integer solution t since p does not divide $f'(x_0)$. Therefore we obtain that $f(x_0 + tp) \equiv 0 \pmod{p^2}$. One can continue in the same way, and thus one proves the first part of our theorem.

b) Suppose now that $f(x)$ and $f'(x)$ are coprime. Then there exist polynomials with rational coefficients $u(x)$ and $v(x)$ such that $u(x)f(x) + v(x)g(x) = 1$. (In order to prove that consider the Euclid's algorithm for division of polynomials, and apply it twice; once climbing down and then climbing up the "staircase".) This means that one can choose u and v with integer coefficients but then one has to substitute the constant 1 by another integer. Let the respective identity be

$U(x)f(x) + V(x)f'(x) = m$ where $m \in \mathbb{N}$. If p is prime such that p divides both $f(x_0)$ and $f'(x_0)$ for some $x_0 \in \mathbb{Z}$ then p must divide m. Hence there are finitely many possibilities for such p, namely the prime divisors of m, and we are done.

Finally we would like to propose to the reader one "generalisation" of the Chinese Remainder Theorem, and a related story. Further generalisations (yes without the quotation marks) can be found in [4].

Exercise 5 *Let a_i, b_i, m_i be integers, and form the system of congruences* | $a_i x \equiv b_i \pmod{m_i}$, *$i = 1, 2, \ldots, n$. Prove that this system has solution if and only if for every two indices $i \neq j$, the system of two congruences $a_i x \equiv b_i \pmod{m_i}$, $a_j x \equiv b_j \pmod{m_j}$ has a solution.*

Solution. Use an induction on n starting with $n = 2$, and "imitate" the proof of the Chinese Remainder Theorem.

Notice that in essence the last exercise states the following. If we are given n arithmetic progressions (infinite at both sides) consisting of integers, then these progressions have a common point of intersection if and only if every two of them have such point.

One interesting question concerns coverings of the integers by arithmetic progressions. One asks whether it is possible to find arithmetic progressions such that every integer belongs to some of them. Of course this question has trivial answer "yes" since the progression $0 + m.1$, $m \in \mathbb{Z}$ covers all integers. Thus let us modify our question. We shall require that our progressions have differences $d_i > 1$. This means our progressions will be of the form $a_i + nd_i$, $n = 1, 2, \ldots$, where $d_i > 1$. But in this case the answer is still trivial: one considers the odd and the even numbers. One is thus led to consider progressions with pairwise distinct differences $d_i > 1$. And our problem becomes the following.

Do there exist a positive integer k and k arithmetic progressions $a_i + d_i b_i$ consisting of integers, where $1 < d_1 < \cdots < d_k$ such that every integer belongs to some of these progressions?

This problem can be easily translated to the language of congruences. In fact it asks whether there exists a collection of congruences $x \equiv a_i \pmod{d_i}$ such that every integer z is a solution for at least one of these congruences.

One easily verifies that when $k = 2$ this is impossible. The case $k = 3$ is easy to eliminate as well. We sketch how to show that the case $k = 4$ is impossible, too. The numbers 1 and 2 belong to two different progressions. If 3 belongs to the first (the one that contains 1) then it consists of all odd integers. Hence 4 cannot belong to the second progression — otherwise the first two progressions would have equal differences. Thus 4 must belong to the third progression. Consider 6 — it cannot belong to the third progression. Now there are two cases to deal with.

a) The number 6 belongs to the second progression. Then the first two are determined, they are 1, 3, 5, 7, …, and 2, 6, 10, 14, … The number 8 does not belong to the third progression; otherwise it would have difference 4. Hence 8 is in the fourth progression. Then 12 is in the second, and the second progression is 4, 12, 20, 28, …, and then 16 must be in the fourth. But this determines it, and it is 8, 16, 24, …, and the difference is 8.

b) The number 6 belongs to the fourth progression. Then consider 8, and continue as in the case (a).

If 3 belongs to the third progression, the considerations are fairly similar to the above, and we leave them to the reader.

Theorem 3 *There exist five arithmetic progressions of integers having differences* $1 < d_1 < d_2 < d_3 < d_4 < d_5$ *that cover the integers.*

Proof. It is sufficient to point out such progressions. We leave to the reader to verify that the five progressions $2k$, $3k+1$, $4k+3$, $6k+5$, and $12k+9$ do cover the integers. (It is sufficient to consider only the integers from 1 to 24 and to prove the statement for them since the differences divide 24).

3 Exercises

Exercise 6 *Solve the system:*

$$a)\ \left|\begin{array}{lll} 5x & \equiv -1 & \pmod{24} \\ 4x & \equiv 19 & \pmod{21} \end{array}\right. ;\ b)\ \left|\begin{array}{lll} 3x & \equiv 7 & \pmod{10} \\ 2x & \equiv 5 & \pmod{15} \\ 7x & \equiv 5 & \pmod{12} \end{array}\right. ;\ c)\ \left|\begin{array}{lll} 4x & \equiv 1 & \pmod{9} \\ 5x & \equiv 3 & \pmod{7} \\ 4x & \equiv 5 & \pmod{12} \end{array}\right.$$

Exercise 7 *Find the least positive integer k such that k divided by 7, 5, 3, 11, yields residues 3, 2, 1, 9, respectively.*

Exercise 8 *Find the least k such that $45 \mid (2^k - 1)$. (Hint: Find the integers m such that $9 \mid 2^m - 1$ and n such that $5 \mid 2^n - 1$.)*

Exercise 9 *Find the digits x and y in the number $n = \overline{4x87y6}$ (in decimal system) if n is divisible by 56.*

Exercise 10 *a) Prove that if $2^n - 1$ is prime then n is also prime.*

b) Prove that for every $n \in \mathbb{N}$ there exist n consecutive terms of the sequence $a_k = 2^k - 1$ that are composite.

Exercise 11 *Let $a+bm$, $m = 1, 2, \ldots$, be an arithmetic progression, and let $n \in \mathbb{N}$. Prove that:*

a) There exist n consecutive terms of the progression such that every one of them is divisible by 2000 distinct primes, and all these $2000.n$ primes are pairwise distinct.

b) Let $k \in \mathbb{N}$ and let $\alpha_i = (i_1, i_2, \ldots, i_k)$ be k-tuples of positive integers, $i = 1$, 2, ..., n. Fix pairwise distinct primes $\{p_{ij} \mid i = 1, 2, \ldots, n; j = 1, 2, \ldots, k\}$. Prove that there exist n consecutive terms of our progression such that the i-th of them is divisible by $p_{i1}^{i_1}$, $p_{i2}^{i_2}$, ..., $p_{ik}^{i_k}$.

c) Is it possible to choose n consecutive terms of our progression that satisfy (b) and satisfy further the condition that neither $p_{ij}^{i_j+1}$ divides the i-th term?

Exercise 12 *Prove that there exist infinitely many primes of the form:*

a) $4n+1$; *b)* $4n+3$; *c)* $6n+1$; *d)* $6n+5$, $n \in \mathbb{N}$.

Hint. Simulate Euclid's proof of the infinity of the primes. For a), suppose that p_1, $p_2, \ldots, p_k$ are the only primes of this form, and set $p = (2p_1p_2 \ldots p_k)^2 + 1$. Using Fermat's Little theorem prove that if a prime $q = 4m + 3$ divides $a^2 + b^2$ then q divides a and b. Another, similar approach to this question is the following. We know that the polynomial congruence $x^2 + 1 \equiv 0 \pmod{p}$ has solution for an infinity of primes p. Of course these cannot be of the form $4m + 3$. But every odd prime is either of the form $4m + 1$ or $4m + 3$.

The statement of b) is easy to prove since product of integers of the form $4s + 1$ is again of the same form. In order to prove c) and d) one uses similar reasoning. (Recall that Fermat's Theorem states that if p is prime then $a^p \equiv a \pmod{p}$. One proves this assertion by induction on a, or by using the fact that all binomial coefficients in the expansion $(x + y)^p$ are divisible by p. One can rewrite the assertion as follows. If p is prime and p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$).

Exercise 13 *Let $f_1, f_2, \ldots, f_n$ be nonconstant polynomials with integer coefficients. Prove that there exist infinitely many $m \in \mathbb{Z}$ such that the integers $f_1(m)$, $f_2(m)$, $\ldots$, $f_n(m)$ are composite.*

Hint. Choose primes p_i and q_i, $i = 1, 2, \ldots, n$ that are pairwise distinct, and such that every one of the congruences $f_i(x) \equiv 0 \pmod{p_i}$, $f_i(x) \equiv 0 \pmod{q_i}$ has solution. Then apply the Chinese Remainder Theorem using the fact that $a \equiv b \pmod{m}$ implies $f(a) \equiv f(b) \pmod{m}$.

Exercise 14 *Let $f(x)$ be nonconstant polynomial with integer coefficients, and let $k \in \mathbb{N}$ and $\alpha_i = (i_1, i_2, \ldots, i_k)$ be k-tuples of positive integers, $i = 1, 2, \ldots, n$. Fix pairwise distinct primes $\{p_{ij} \mid i = 1, 2, \ldots, n; j = 1, 2, \ldots, k\}$. Prove that there exist n consecutive positive integers $x + i$, $i = 1, 2, \ldots, k$, such that $f(x + i)$ is divisible by $p_{i1}^{i_1}, p_{i2}^{i_2}, \ldots, p_{ik}^{i_k}$ for every i.*

Exercise 15 *Is it possible to choose in the previous exercise, the integers $x + i$, $i = 1, 2, \ldots, k$ such that neither $p_{ij}^{i_j+1}$ divides $f(x + i)$? Consider at least the case when f is irreducible.*

Exercise 16 *Let $b > 1$ and c be integers, and let $x_n = b^n + c$. Prove that:*

a) The congruence $x_n \equiv 0 \pmod{p}$ has solution for infinitely many primes p;

b) There exist infinitely many composite numbers in the sequence $\{x_n\}$;

c) Generalize (a) and (b), for the function $g(x) = ab^x + c$ where $a, b \in \mathbb{N}$, $c \in \mathbb{Z}$.

Hint. Elaborate the following reasoning. If $p_1, \ldots, p_n$ are primes then due to Fermat Little theorem one has $a^{s(t)} \equiv a \pmod{p_1 \ldots p_n}$ where $s(t) = t(p_1 - 1) \ldots (p_n - 1) + 1$, $t \in \mathbb{N}$.

References

[1] **Anglin, W.S.**, *The queen of mathematics. An introduction to number theory*, Kluwer Texts in Math. Sciences 8, Kluwer, Dordrecht, 1995.

[2] **Coutinho, S.C.**, *Números Inteiros e Criptografia RSA*, IMPA/SBM, Série de Computação e Matemática, Rio de Janeiro, 1997.

[3] **Godinho, H., Soares, M. and Shokranian, S.**, *Introdução à Teoria dos Números*, 2^a. ed., Ed. UnB, Brasília, 1998.

[4] **Ireland, K. and Rosen, M.**, *A classical introduction to modern Number theory*, Springer-Verlag, New York, 1982.

[5] **Matiyasevich, Yu. V.**, *Hilbert's tenth problem*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993.

[6] **Niven, I., Zuckerman, H. and Montgomery, H.**, *An introduction to the theory of numbers*, Wiley, New York, 1991 (Fifth edition).

[7] **Rose, H.E.**, *A course in number theory*, Oxford Science Publ., Clarendon Press, Oxford Univ. Press, New York, 1988.

[8] **Sierpiński, W.**, *250 problems in elementary Number theory*, Elsevier, New York and PWN, Warszawa, 1970.