SOLVING THE CONGRUENCE $\mathbf{P(x) \equiv 0 \bmod N}$.

Dmitry FUCHS

A lot is said and written about solving algebraic equations $P(x) = 0$ where P is a polynomial. We will consider today a seemingly similar, but actually very much different problem. We suppose that P is a polynomial with *integer* coefficients, and want to find those *integers* x for which $P(x)$ is *divisible by* N.

1. A preparation. We will begin with several statements which are not related directly to our problem, but will be useful to us. Probably, the members of the circle are familiar with all, or almost all, of them, but I feel obliged to walk through them.

First, the notation (it, actually, was used in the title): for integers a, b, and $n > 0$, the formula $a \equiv b \bmod n$ (read as "a is congruent to b modulo n") means "$a - b$ is divisible by n". For example, $17 \equiv 9 \bmod 4$, $-12 \equiv 2 \bmod 7$, but $16 \not\equiv 8 \bmod 5$. In particular, $a \equiv 0 \bmod n$ means that a is divisible by n. Mark the following obvious properties of congruences: if $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a+c \equiv b+d \bmod n$, $a-b \equiv b-d \bmod n$, and $a \cdot c \equiv b \cdot d \bmod n$.

Second, if we do not distinguish between integers congruent modulo n, then there will be precisely n "different" numbers: $0, 1, 2, \dots, n-1$. I mean that any integer is congruent modulo n to precisely one of these numbers. In connection with this, we will use the word "residue": if a is congruent modulo n to $b, 0 \leq b \leq n-1$, then we will say that b is the *residue* of a modulo n. (In particular, each of the numbers $0, 1, \dots, n-1$ is the residue of its own.) We can *add, subtract* and *multiply* residues. For example, the residue of $4+5$ modulo 7 is 2, so we say, that the residue 2 is the sum of the residues 4 and 5 modulo 7. Similarly, the residue 6 is the product of the residues 4 and 5 modulo 7.

Third, there is such a thing as division modulo a prime number. Let p be a prime (number), and let a and b are integers such that a is not divisible by p. Then it is possible to "divide a by b modulo p. More precisely: *there exists a unique modulo p integer c such that $a \cdot c \equiv b \bmod p$.* Indeed, consider the integers

$$0 \cdot a, 1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a. \qquad (*)$$

The number of this integers is p, and no two of them have the same residue modulo p (if $k \cdot a \equiv \ell \cdot a \bmod p$ and $0 < \ell < k < p$, then $(k - \ell) \cdot a$ is divisible by p; since p is prime and a is not divisible by p, then $k - \ell$ should be divisible by p, which is obviously not possible). Since there are precisely p different residues modulo p, there is, among the residues $(*)$ precisely one, which coincides with the residue of b. For example, how to divide 3 by 5 modulo 7? We consider the 7 integers $0, 5, 10, 15, 20, 25, 30$ and locate the one of them which is congruent to 3 modulo 7. It is $10 = 2 \cdot 5$. Thus, the result of division of 3 by 5 modulo 7 is 2.

To make this computation simpler, we can find the "inverse" residues: 1 divided by all the other non-zero residues; if p is fixed, we may use for the residue "1 divided by the residue a" the "bar-notation" $\overline{a}$. For example, modulo 7, $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ are $1, 4, 5, 2, 3, 6$; modulo 11, $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}$ are $1, 6, 4, 3, 9, 2, 8, 7, 5, 10$. If we know this, we can divide any residue (modulo a prime) by any non-zero residue: to divide b by a is the same as to multiply b by $\overline{a}$. For example, let us divide 5 by 7 modulo 11. Since $\overline{7} = 8$, it is the same as multiply 5 by 8 modulo 11. But $5 \cdot 8 = 40 \equiv 7 \bmod 11$, so the result of division is 7. (Indeed, $7 \cdot 7 = 49 \equiv 5 \bmod 11$.)

A couple of additional remarks not concerning congruences. Let $P(x)$ be a polynomial with integer coefficients,

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0.$$

Then the *derivative* of $P(x)$,

$$P'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2x + a_1$$

is also a polynomial with integer coefficients. The same is true for the *second derivative*,

$$P''(x) = n(n-1)a_nx^{n-2} + (n-1)(n-2)a_{n-1}x^{n-3} + \ldots + 6a_3x + 2a_2,$$

but actually we have more: all the coefficients of this polynomial are *even* (since all the numbers $\dfrac{k(k-1)}{2} = \dbinom{k}{2}$ are integers); thus, not only $P''(x)$, but also $\dfrac{P''(x)}{2}$ is a polynomial with integer coefficients. Similarly, all the coefficients of the polynomial

$$P'''(x) = n(n-1)(n-2)a_nx^{n-2} + (n-1)(n-2)(n-3)a_{n-1}x^{n-3} + \ldots + 24a_4x + 6a_3$$

are divisible by $3! = 6$, so $\dfrac{P'''(x)}{3!}$ is a polynomial with integer coefficients, and so on: $\dfrac{P^{(k)}(x)}{k!}$ (where $P^{(k)}(x)$ denotes the k-th derivative of the polynomial $P(x)$) is, for every k, a polynomial with integer coefficients.

And the last thing I want to mention here is the *Taylor formula*: for a polynomial $P(x)$,

$$P(a+h) = P(a) + P'(a)h + \frac{P''(a)}{2}h^2 + \frac{P'''(a)}{3!}h^3 + \ldots$$

This formula is well known in elementary calculus. It is important that for polynomials the sum in the right hand side has finitely many terms: for a degree n polynomial $P(x)$ the derivatives starting with the $(n+1)$-st one are all zeroes. (For those who do not know this formula, here is a brief proof. Since every polynomial is the sum of powers x^n with some coefficients, it is sufficient to prove it for the polynomial $P(x) = x^n$. For this polynomial,

$$P(a+h) = (a+h)^n = a^n + na^{n-1}h + \frac{n(n-1)}{2}a^{n-2}h^2 + \frac{n(n-1)(n-2)}{3!}a^{n-3}h^3 + ...$$

But $a^n = P(a)$, $na_{n-1}a^{n-1} = P'(a)$, $n(n-1)a_{n-2}a^{n-2} = P''(a)$, $n(n-1)(n-2)a_{n-3}a^{n-3} = P'''(a)$, and so on, so our formula holds in this case.)

2. The problem. Let $P(x)$ be a polynomial with integer coefficients, and let $N \geq 2$ be an integer. We are looking for those integers x for which $P(x) \equiv 0 \bmod N$. First of all, it is obvious that if x is a solution of our problem and $y \equiv x \bmod N$, then y is also a solution of our problem. Thus, our solutions will be residues modulo N; it is possible to say that we are looking for solutions only among the numbers $0, 1, 2, \ldots, N-1$. What can be the number of solutions? We can say only that if N is prime that the number of solutions cannot exceed the degree of the polynomial. (We do not need this fact, and will not prove it, but the proof is the same as in elementary algebra; we need to use the division modulo p, then we prove that if $P(x)$ has degree n and $P(a) \equiv 0 \bmod p$, then, modulo p, $P(x) = (x-a) \cdot Q(x)$ where $Q(x)$ is a polynomial of degree $n-1$ less the degree of $P(x)$; we can assume, by induction, that the congruence $Q(x) \equiv 0 \bmod p$ has at most $n-1$ solutions, and the congruence $P(x) \equiv 0 \bmod p$ has the same solutions and also a.) If N is not prime, then the number of solutions may exceed the degree of the polynomial; for example, the congruence $x^2 - 1 \equiv 0 \bmod 8$ has 4 solutions: 1, 3, 5, and 7.

3. A Chinese contribution. One of the oldest results in Number Theory is the so-called Chinese Remainder Theorem*. For example, consider the following problem; find all integers x such that $x \equiv 3 \bmod 5$ ands $x \equiv 2 \bmod 7$. One of solutions is 23, and this is a unique solution modulo $5 \cdot 7 = 35$; so all solutions are $\ldots, -12, 23, 58, 91, \ldots$, that is, $23 + k \cdot 35$ where k is an arbitrary integer. The theorem says that if k and ℓ are relatively prime, then, for arbitrary a and b, the system of congruences $x \equiv a \bmod k$, $x \equiv b \bmod \ell$ has a unique solution modulo mn. (The proof is basically the same as for the existence of division modulo a prime. We consider integers

$$a,\ a+k,\ a+2k,\ a+3k, \ldots, a+(\ell-1)k.$$

All of them satisfy the first congruence, there are ℓ of them, and all of them have different residues modulo ℓ. Indeed, if $0 \le s < t \le \ell - 1$, then if $(a+tk) - (a+sk) = (t-s)k$ were divisible by ℓ, then, since k and ℓ are relatively prime, $t-s$ would be divisible by ℓ which is not possible: $0 < t-s < \ell$. Hence all the ℓ numbers have different residues modulo ℓ, and, since there are precisely ℓ different residues modulo ℓ, there precisely one s, $0 \le s \le \ell - 1$ such that the residue of $a + sk$ modulo ℓ is b: this provides a unique modulo $k\ell$ solution to our system: $a + sk$.

Now, if our N is a product of two relatively prime numbers, $N = k\ell$, then any y and z such that $P(y) \equiv 0 \bmod k$ and $P(z) \equiv 0 \bmod \ell$ produce a solution modulo N: it is sufficient to take an x such that $x \equiv y \bmod k$ and $x \equiv z \bmod \ell$. Indeed, since $P(x)$ is divisible by k and by ℓ, it is also divisible by $k\ell = N$.

Now, an arbitrary N has a prime factorization: $N = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_r^{k_r}$, where $p_1, p_2, p_3, \ldots, p_r$ are different prime numbers. Since $p_1^{k_1}$ is relatively prime to $p_2^{k_2} p_3^{k_3} \ldots p_r^{k_r}$, it is sufficient to solve the problem modulo $p_1^{k_1}$ and $p_2^{k_2} p_3^{k_3} \ldots p_r^{k_r}$. Since $p_2^{k_2}$ is relatively prime with $p_3^{k_3} \ldots p_r^{k_r}$, It is sufficient to solve the problem modulo $p_1^{k_1}$, $p_2^{k_2}$ and $p_3^{k_3} \ldots p_r^{k_r}$; and so on. The final result: we need to solve our problem modulo $p_1^{k_1}$, $p_2^{k_2}$, $\ldots$, $p_r^{k_r}$: every set of solutions of these r problems will provide a unique, modulo N solution of the congruence modulo N.

* Why this name? Different sources provide different explanations for this. One states that the name of the discoverer is too difficult for pronunciation. Another explanation, which seems more plausible to me, states that the fact was known in China many centuries ago, but it is difficult to find out who was the first discoverer.

We arrive at a conclusion: the only case we need to consider is the case when N is a power of prime.

From now on, we fix a prime number p and assume that N is a power of p.

4. The case of prime N. First, we need to consider the case when N is p. This case, which may seem the easiest, is actually the most difficult. I can say that there are no sophisticated means to solve the congruence $P(x) \equiv 0 \bmod p$. All we can offer is to plug for x, one by one, the numbers $0, 1, 2, \dots, p-1$. (It may be helpful to know that the number of solutions does not exceed the degree of $P(x)$.) If p is not very big, we can do this by hand; for a bigger p, we can use a simple computer program. For example, it is not hard to check by a manual computation that the congruence $n^3 + 4n + 2 \equiv 0 \bmod 7$ has 2 solutions (modulo 7): 1 and 5. The congruence $n^3 + 4n + 2 \equiv 0 \bmod 101$ has a unique (modulo 101) solution: $x = 37$; but I was able to find it only with the help of a computer.

5. The transition $\mathbf{N = p^k \to N = p^{k+1}}$ ($\mathbf{k \geq 1}$): Hensel's Lemma, the statement. Obviously, a solution of the congruence $P(x) \equiv 0 \bmod p^{k+1}$ is also a solution of the congruence $P(x) \equiv 0 \bmod p^k$. So, our problem may be stated in the following way. Let x be a solution of the congruence $P(x) \equiv 0 \bmod p^k$. Find the solutions of the congruence $P(y) \equiv 0 \bmod p^{k+1}$ such that $y \equiv x \bmod p^k$. If $0 \leq x < p^k$, then there are p integers y such that $y \equiv x \bmod p^k$ and $0 \leq y < p^{k+1}$: these are $x, x + p^k, x + 2p^k, \dots, x + (p-1)p^k$. So, our problem takes the following form: for a solution x of the congruence $P(x) \equiv 0 \bmod p^k$, find all integers $a, 0 \leq a \leq p-1$ such that $P(x + ap^k) \equiv 0 \bmod p^{k+1}$. For $k \geq 1$, this problem is solved by the following beautiful theorem which is known as *Hensel's Lemma.*

Hensel's Lemma. *Let $P(x)$ be a polynomial with integer coefficients, and let p be a prime. Further, let $k \leq 1$, and let $P(x) \equiv 0 \bmod p^k$, $0 \leq x < p^k$. There are two cases.*

Case One*: $P'(x) \not\equiv 0 \bmod p$. Then there exists a unique $a, 0 \leq a \leq p-1$ such that $P(x + ap^k) \equiv 0 \bmod p^{k+1}$. More precisely, a is obtained by the division of the residue modulo p of the integer $P(x)/p^k$ by the residue modulo p of $-P'(x)$.*

Case Two*: $P'(x) \equiv 0 \bmod p$. Then there are two possibilities: either $P(x + ap^k) \equiv 0 \bmod p^{k+1}$ for all a between 0 and $p-1$, or this holds for no one of these a.*

6. Proof of Hensel's Lemma. It is sort of unfair that the proof of this remarkable theorem is so simple.

Proof (Case One). By the Taylor formula (see Section 1),

$$P(x + ap^k) = P(x) + P'(x) \cdot ap^k + \underbrace{\frac{P''(x)}{2} \cdot (ap^k)^2 + \frac{P'''(x)}{3!} \cdot (ap^k)^3 + \dots}_{\text{divisible by } p^{k+1}}$$

[Here we use the fact that $\dfrac{P^{(k)}(x)}{k!}$ is an integer (see Section 1) and also the inequality $k \geq 1$: it implies the inequality $2k \geq k + 1$.] Thus, the congruence $P(x + ap^k) \equiv 0 \bmod p^{k+1}$ is equivalent to the congruence $P(x) + P'(x) \cdot ap^k \equiv 0 \bmod p^{k+1}$, which, in turn, is equivalent to the congruence $\dfrac{P(x)}{p^k} + P'(x) \cdot a \equiv 0 \bmod p$. Thus, a (which may be considered as a residue modulo p) is uniquely defined and is obtained by the residue division as described in the statement.

(Case Two.) If $P'(x) \equiv 0 \bmod p$, then the same Taylor formula shows that, independentlly of a, $P(x + ap^k) \equiv P(x) \bmod p^{k+1}$, which implies our statement.

7. How it works. We choose a solution x_0, $0 \leq x_0 < p$ of the congruence $P(x) \equiv 0 \bmod p$. Suppose that $P'(x_0)$ is *not* divisible by p. In this case, we change the notation x_0 to a_0. A successive application of the Case One of Hensel's Lemma gives the following:

there exists a unique a_1, $0 \leq a_1 < p$ such that $P(a_0 + a_1 p) \equiv 0 \bmod p^2$;
there exists a unique a_2, $0 \leq a_1 < p$ such that $P(a_0 + a_1 p + a_2 p^2) \equiv 0 \bmod p^3$;
there exists a unique a_3, $0 \leq a_1 < p$ such that $P(a_0 + a_1 p + a_2 p^2 + a_3 p^3) \equiv 0 \bmod p^4$;

and so on. Moreover, all these a_i's are described by explicit formulas. Notice also that all $P'(a_0), P'(a_0 + a_1 p), P'(a_0 + a_1 p + a_2 p^2), \ldots$ are the same modulo p; so, to find the whole sequence $a_1, a_2, a_3, \ldots$ we need only to find the residue $b = \overline{(-P'(a_0))}$ and then use the formulas

$$a_1 = [P(a_0)/p]_p \cdot b,\ a_2 = [P(a_0 + a_1 p)/p^2]_p \cdot b,\ a_3 = [P(a_0 + a_1 p + a_2 p^2)/p^3]_p \cdot b,$$

($[z]_p$ denotes the residue of z modulo p, and $\cdot$ denotes the multiplication of residues) and so on.

Suppose now that $P'(x_0)$ is divisible by p. If $P(x_0)$ is not divisible by p^2, then it is a dead end: no congruence $P(x) \equiv 0 \bmod p^k$ with $k \geq 2$ will have no solutions congruent to x_0 modulo p. If, however, $P(x_0)$ is divisible by p^2, then the congruence $P(x) \equiv 0 \bmod p^2$ acquires p different (modulo p^2) solutions congruent to x_0 modulo p: $x_0, x_0 + p, x_0 + 2p, \ldots, x_0 + (p-1)p$. We will have to check each of $P(x_0 + ap)$ for the divisibility by p^3; those of them, which are divisible by p^3, provide p solutions of the congruence $P(x) \equiv 0 \bmod p^3$. And so on.

We see that applications of Case Two meet more difficulties that those of Case One. Below, we will use mostly Case One.

8. An example. Let $P(x) = x^3 + 4x + 2$ and $p = 7$. Then $P(0) = 2$, $P(1) = 7$, $P(2) = 18$, $P(3) = 41$, $P(4) = 82$, $P(5) = 147$, $P(6) = 242$. Of all this numbers, only $P(1)$ and $P(5)$ are divisible by 7; thus, the congruence $P(x) \equiv 0 \bmod 7$ has two solutions: 1 and 5. Furthermore, $P'(x) = 3x^2 + 4$, $P'(1) = 7 \equiv 0 \bmod 7$, $P'(5) = 79 \equiv 2 \bmod 7$.

Let us begin with a remark that since $P(1)$ is not divisible by $7^2 = 49$, Case Two of Hensel's Lemma says, basically, that we can forget of this solution: no congruence $P(x) \equiv 0 \bmod 7^k$ with $k \leq 2$ has any solution congruent to 1 modulo 7.

It is all very different with 5. Since $\overline{(-P'(5))} = \overline{(-2)} = 3$, we have the following:

$P(5) = 147$, $147/7 = 21 \equiv 0 \bmod 7$, $a_1 = 0 \cdot 3 = 0$;
$5 + 0 \cdot 7 = 5$, $P(5) = 147$, $P(5)/7^2 = 3$, $a_2 = 3 \cdot 3 = 2$;
$5 + 2 \cdot 7^2 = 103$, $P(103) = 1093141$, $P(103)/7^3 = 3187 \equiv 2 \bmod 7, a_3 = 2 \cdot 3 = 6$;
$103 + 6 \cdot 7^3 = 2161$, $P(2161) = 100917079$, $P(2161)/7^4 = 4203127 \equiv 5 \bmod 7$,
$a_4 = 5 \cdot 3 = 1$;

$P(5+0\cdot 7+2\cdot 7^2+6\cdot 7^3+7^4)/7^5 = 5649054 \equiv 5 \bmod 7$, $a_5 = 5\cdot 3 = 1$;
$P(5+0\cdot 7+2\cdot 7^2+6\cdot 7^3+7^4+7^5)/7^6 = 82940063 \equiv 3 \bmod 7$, $a_6 = 3\cdot 3 = 2$;
$P(5+0\cdot 7+2\cdot 7^2+6\cdot 7^3+7^4+7^5+2\cdot 7^6)/7^7 = 20531648631 \equiv 4 \bmod 7$, $a_7 = 4\cdot 3 = 5$.

Thus, $a_0, a_1, \dots, a_7$ are $5, 0, 2, 6, 1, 1, 2, 5$, so

$$P(5+0\cdot 7+2\cdot 7^2+6\cdot 7^3+1\cdot 7^4+1\cdot 7^5+2\cdot 7^6+5\cdot 7^7) \equiv 0 \bmod 7^8.$$

I found the numbers a_0 and a_1 manually; for a_2 I had to use a pocket calculator; the numbers $a_3, \dots, a_7$ required a simple computer program. Certainly, using more sophisticated instruments, we can find the numbers a_i much farther. These numbers form an infinite sequence of residues modulo 7. What is this sequence?

The solutions modulo 7^k are $5, 5+2\cdot 7^2, 5+2\cdot 7^2+6\cdot 7^3$, and so on. This integers have obvious representation in the numerical system with the base 7: $5_7, 205_7, 6205_7$, and so on. But we have nothing to be called the *limit* of this sequence.

It often happens that when mathematician do not understand the nature of some phenomenon, they just invent a name for it; after this, they feel themselves more confident with the phenomenon. We consider an infinite series $5+0\cdot 7+2\cdot 7^2+6\cdot 7^3+1\cdot 7^4+1\cdot 7^5+2\cdot 7^6+5\cdot 7^7+\dots$ and call it a *p-adic integer.* Thus, a p-adic integer is a "number with infintely many digits," in our case, $\dots 52116205_7$. If the sequence of digits is finite (that is, starting from some moment, they are all zeroes), then a p-adic integer is a genuine non-negative integer. In general, p-adic integers have residues modulo p, p^2, p^3, and so on, and the residue modulo p^{k+1} is congruent modulo p^k to the residue modulo p^k. The difference between a general p-adic integer and a non-negative integer is that for a non-negative integer this sequence of residues stabilizes (for example, for $n = 500$, the sequence of residues modulo $7, 7^2, 7^3, \dots$ is $3, 10, 157, 500, 500, 500, \dots$, while for a general p-adic integer no such stabilization holds.

The Case One of Hensel's Lemma states that if a_0, $0 \le a_0 < p$, is a solution of a congruence $P(x) \equiv 0 \bmod p$ and $P'(a_0) \not\equiv 0 \bmod p$, then there exists a unique p-adic solution of the equation $P(x) = 0$ whose residue modulo p is a_0.

9. p-adic arithmetic. The last statement means that we can "plug" a p-adic integer into a polynomial with integral coefficients. This requires some understanding of the p-adic arithmetic.

Question One: can we add p-adic integers? Answer: why not? For p-adic integers, the addition is not different from the usual elementary school addition. Say, let us find the sum of 7–adic integers $\dots 365044$ and $\dots 264535$:

$$\begin{array}{cr} & {\scriptstyle 1\;1\;\;\;\;1\;1\;\;\;} \\ & \cdots 365044 \\ + & \cdots 264535 \\ \hline & \cdots 662612 \end{array}$$

We begin from the left. The leftmost digits are 4 and 5, $4+5 = 9$, the residue modulo 7 is 2. We wright 2 and, for the remaining 7, carry a 1 to the nest digits to the right. For these next digits, we have $1+4+3 = 8$, the residue is 1, we write 1 and again carry 1 to the next digit to the right. For the next digits, we have $1+0+5 = 6$, we write 6 and carry nothing. Next, $5+4 = 9$, we write 2 and carry 1. Next: $1+6+6 = 13$, we write 6 and carry 1. Next digits: $1+3+2 = 6$, we write 6. And so on.

Question Two: can we subtract p-adic integers? Yes, and all we need for that is to subtract an arbitrary p-adic number from zero. If we have a p-adic integer $\ldots a_3a_2a_1a_0$ and $a_0 \neq 0$, then the “subtraction from zero” gives $\ldots b_3b_2b_1b_0$ where $b_0 = p - a_0$, $b_1 = p-1-a_1$, $b_2 = p-1-a_2, b_3 = p-1-a_3$ and so on. The addition $\ldots a_3a_2a_1a_0 + \ldots b_3b_2b_1b_0$ gives obviously $\ldots 0000$ (we carry 1’s at every step). (Example for $p = 7$: $0 - \ldots 264535 = \ldots 402132$.) What to do, if $a_0 = 0$? Let $a_0 = a_1 = \ldots = a_{k-1} = 0$ and $a_k \neq 0$. Then we put $b_0 = b_1 = \ldots = b_{k-1} = 0$ and $b_k = p - a_k$, $b_{k+1} = p - 1 - a_{k+1}$, $b_{k+2} = p - 1 - a_{k+2}$, and so on. (We need to say also that zero minus zero is zero.) To complete the definition of subtraction, we say that $A - B = A + (0 - B)$.

Notice that there is no such things as *positive* and *negative* p-adic integers (although there is a zero); still, the subtraction is always possible.

Question Three: what about the multiplication? Again, elementary school students are ready to help. Let us try to multiply the two 7-adic integers, which we used in our example of addition.

$$\begin{array}{rl}
 & \cdots 365044 \\
\times & \cdots 264535 \\
\hline
 & \cdots 554316 \\
 & \cdots 61165 \\
 & \cdots 4316 \\
 & \cdots 242 \\
 & \cdots 63 \\
 & \cdots 1 \\
\hline
 & \cdots 533166
\end{array}$$

Let us explain this. First we muptiply $\ldots 365044$ by the last digit of the second factor, that is, by 5. We take the product $5 \times 4 = 20$, it is 6 modulo 7: $20 = 6 + 2 \cdot 7$, we write 6 and “carry” 2. Then we multiply 5 by the second digit of $\ldots 365044$, that is, again, by 4, and add our “carry”: $5 \times 4 + 2 = 22$, it is 1 modulo 7: $22 = 1 + 3 \cdot 7$, so we right 1 next to 6 and carry 3. Next step: $5 \cdot 0 + 3 = 3$, we write 3 next to 1 and “carry” nothing. Then $5 \cdot 5 + 0 = 25$, we write 4 and carry 3; and so on. In this way we form the “first line”: $\ldots 554316$. Then we multiply, in the same way, 3 by $\ldots 365044$ and write the result as the second line with a shift to the left by one position: $\ldots 61165$. And so on. Then we add up the lines, as they are written, and obtain the desired product.

We see that the product of two p-adic integers is well defined. Obviously, zero times anything is zero, one times anything is this anything. It requires some efforts to check that the multiplication is commutative, associative and distributive. Also, it is true that the operation of subtraction from zero (described above) is the same as the multiplication by “negative one,” which is $\ldots (p-1)(p-1)(p-1)(p-1)$. These statements may be regarded as exercises.

The last funny remark: what happens, if we multiply a p-adic integer $A = \ldots a_3a_2a_1a_0$ by p? It is easy: the integer p, as a p-adic integer, is $\ldots 00010$, so the multiplication gives the same A shifted by one position to the left: $\ldots a_3a_2a_1a_00$. Another explanation: $(\ldots + a_3p^3 + a_2p^2 + a_1p + a_0) \times p = \ldots + a_3p^4 + a_2p^3 + a_1p^2 + a_0p + 0$.

Question Four: division. This is a delicate question. In the usual arithmetic, the division of an integer by an integer is not always possible (within the domain of integers; mathematicians, following the recommendation given above, solve the problem by inventing a new name: a *rational number*, or a *fraction*). Say, we can divide 102 by 3, but cannot divide 101 by 3. This leads to a huge (actually, never ending) variety of divisibility rules. For p-adic integers, the situation is much simpler: *if $A = \ldots a_4a_3a_2a_1a_0$ and $B = \ldots b_4b_3b_2b_1b_0$ are p-adic integers* **and $\mathbf{a_0 \neq 0}$**, *then B is divisible by A*, that is, there exists a p-adic integer $C = \ldots c_4c_3c_2c_1c_0$ such that $B = A \cdot C$.

We will demonstrate this on an example; we will use the same 7-adic integers, which we used to demonstrate addition and multiplication: we will show how to divide 7-adic $\ldots 264535$ by 7-adic $\ldots 365044$. We want to find a 7-adic integer C such that $\ldots 365044 \cdot C = \ldots 264535$. What is the last digit of C? It is a residue modulo 7 whose product with 4 is 5. The division of 5 by 4 modulo 7 is possible (because $4 \neq 0$) and gives 3. Let us write

$$\begin{array}{lr}
\cdots & 365044 \\
\cdots & 3 \\ \hline
\cdots & 461165
\end{array}$$

The last digit is 6, it is OK, but the next (to the left) digit is 6, while we want to have 3. To compensate this, we need to add 4 to this 6, and 4 divided by 4 (we must say, modulo 7, although it is not important now) is 1. Write 1 next to 3 in the second line and multiply:

$$\begin{array}{lr}
\cdots & 365044 \\
\cdots & 13 \\ \hline
\cdots & 461165 \\
\cdots & 65044 \\ \hline
\cdots & 635
\end{array}$$

Now, the last two digits of the product are 35, this is what we want, but the digit 6 before them is not satsfactory: we want to see 5 there. To turn 6 into 5, we need to add 6 to it. Since 6 divided by 4 modulo 7 is 5, we write 5 before 13 in the second line. Then we multiply:

$$\begin{array}{lr}
\cdots & 365044 \\
\cdots & 513 \\ \hline
\cdots & 461165 \\
\cdots & 65044 \\
\cdots & 4136 \\ \hline
\cdots & 3535
\end{array}$$

Here we encounter the same problem as before: the last three digits of the product, 535, are OK, but the digit 3 before them is not what we want: we want to see 4 there. To compensate this, we need to add 1 to 3; to achieve this, we divide 1 by 4 modulo 7, get 2 and write this 2 before 513 in the second line. And so on. Here is the final result:

$$\begin{array}{l} \cdots 365044 \\ \cdots 412513 \\ \hline \cdots 461165 \\ \cdots 65044 \\ \cdots 4136 \\ \cdots 121 \\ \cdots 44 \\ \cdots 2 \\ \hline \cdots 264535 \end{array}$$

We obtain the 7-adic division: $(\ldots 264535) \div (\ldots 365044) = \ldots 412513$. If you examine the operations involved, you will notice that at every step we had to divide, modulo 7, some digit by 4; all the rest was a plain multiplication. You can see from this example, that every p-adic integer is "divisible" by every p-adic integer (that is, the result of division is also a p-adic integer) provided that the last digit of divisor is not zero. (No division rules!!!)

But what if the last digit of the divisor **is** zero? For example, how to divide $\ldots 264535$ by $\ldots 3650440$? Well, $\ldots 3650440$ is $\ldots 365044$ times $7 = \ldots 000010$. Thus, to divide $\ldots 264535$ by $\ldots 3650440$, we first divide it by $\ldots 365044$ and get $\ldots 412513$ and then want to divide $\ldots 412513$ by $\ldots 000010$, which seems to be impossible. But is it really so? What we want is to divide $\ldots + 4 \cdot 7^5 + 1 \cdot 7^4 + 2 \cdot 7^3 + 5 \cdot 7^2 + 1 \cdot 7 + 3$ by 7. Our common sense says that we should get $\ldots + 4 \cdot 7^4 + 1 \cdot 7^3 + 2 \cdot 7^2 + 5 \cdot 7 + 1 + 3 \cdot 7^{-1}$. It is something like a decimal fraction with one digit after the decimal dot, which we may call a p-mal fraction: $\ldots 41251.3$. We can consider this as a new notation, and using it, we can say that the division of any p-adic integer by any non-zero p-adic integer gives a p-mal fraction with finitely many digits after the p-mal dot. Even more: the ratio between two p-mal fractions, of which the second is not zero, is a p-mal fraction. The number of digits after the p-mal dot is always finite. No infinite p-mal fractions, periodic or not periodic, exist in the p-adic arithmetics: forget about them.

For those who value periodic fractions beyond any ability to forget them, we offer the following exercise: prove that the 7-adic $1 \div 2$ is $\ldots 33334$; a generalization: prove that the p-adic fraction $a \div b$ where a and b are positive (not p-adic!) integers is *periodic to the left*. Two more examples: 7-adic $5 \div 3$ is $\ldots 22224$, and 7-adic $3 \div 5$ is $\ldots \underbrace{1254}\underbrace{1254}\underbrace{1254}2$.

The conclusion which we arrive at: the p-adic arithmetic is much simpler (or, maybe, we should say "much better organized") than the usual arithmetic. And not only this!

10. p-adic algebra. We already have Hensel's Lemma, which paves a way to solving algebraic equations. Let us begin with the simplest application of it: with square roots. Say, what is the 7-adic aquare root of 2? No problems with that: we want to solve, in 7-adic integers, the equation $x^2 - 2 = 0$. This equation has two solutions modulo 7, namely 3 and 4. The derivative of the polynomial $x^2 - 2$ is $2x$, certainly it is not zero for x being either 3 of 4; so, we can find its 7-adic solution whose residue modulo 7 is 3, and this solution is unique. A computation, which looks very much like the computation in Section 8, gives the result: 7-adic square root of 2 is $\ldots 266421216213$. There is also a square root of 2 which ends by the digit 4, we can find it by the same procedure, but also we can say that it is "minus the previous square root," that is, $\dots 400245450454$. Well, a what about a 7-adic square root of 3? Unfortunately, 3 is not a "quadratic residue modulo 7," that is, it is not a square of any other residue modulo 7. So, there is no 7-adic integer (or 7-adic rational number) whose square is 3. I can say that the square root of 3 for 7-adic numbers is the same as the square root of 2 (or of 3) for usual rational numbers: not that it does not exist, but to speak of it, we have to admit that it belongs to an appropriate extension of the realm of p-adic rational numbers (which could be called "p-adic algebraic numbers," but I have never heard this name).

Still I must mention that Case One of Hensel's Lemma has a natural generalization: if an algebraic equation $P(x) = 0$ with integer p-adic coefficients has a solution a_0 modulo p such that $P'(a_0)$ is not divisible by p, then it has a unique integer p-adic solution whose residue modulo p is a_0. The proof of this fact is a replica of the proof of Case One of Hensel's Lemma given in Section 6. By the way, if we had had noticed this before, we could have demonstrated the existence of p-adic division in a very simple way. Look: we want to find a p-adic solution of an equation $Ax - B = 0$ where the last digit of A is not zero. It has a (unique) solution modulo p: it is the usual division modulo p, which we discussed in Section 1. The derivative of $Ax - B$ is A; again, it is not zero modulo p. Hence, the solution exists and is unique.

11. p-adic analysis. I will not say much about it. Almost all major notions of calculus exist in the p-adic context. And, as it is the case for arithmetic and algebra, the p-adic analysis is much "better organized" than the usual analysis. I will mention two examples. In the classical calculus, it is well known that a series $\sum\limits_{n=0}^{\infty} a_n$ diverges unless $\lim\limits_{n\to\infty} a_n = 0$, but the condition $\lim\limits_{n\to\infty} a_n = 0$ is not sufficient for the convergency; this gives rise to multiple convergency tests, and many generations of college students have hated them. But in the p-adic analysis the result is much better looking: a series converges if and only if its terms converge to zero. Another example: in classical analysis a power series $\sum a_n x^n$ has a convergency radius R; the series converges for $|x| < R$, diverges for $|x| > R$ and – nothing is known for $|x| = R$. This is especially important for the power series of complex variable, or of several real variables. Power series in p-adic analysis also have convergency radii, but on the boundary of the convergency interval, or disc, we have a very simple alternative: either the series converges for all x on this boundary, or diverges for all x on this boundary.

There is much more. There exist p-adic geometry, p-adic representation theory, even p-adic field theory, which becomes more and more popular in Mathematical Physics. I stop here, but for those who want to know more, there are books. I will mention two of them; both are attractively short. The first is my favorite, the second is also very well written and addressed, more or less, to people like you.

1. Neal Koblits, "p-adic Numbers, p-adic Analysis, and Zeta-Functions." Graduate Texts in Mathematics, Vol. 58. Springer, 1984.

2. Svetlana Katok, "p-adic Analysis Compared with Real." Student Mathematical Library, Vol. 37. Amer. Math. Soc., 2007.