Michel Waldschmidt *12/11/2013*

SEAMS School 2013 ITB
Number theory

`Exercise 1`
Let $a \geq 2$ and $n \geq 2$ be integers.
a) Assume that the number $N = a^n - 1$ is prime. Show that N is a Mersenne prime, that is $a = 2$ and n is prime.
b) Assume that the number $a^n + 1$ is prime. Show that n is a power of 2, and that a is even. Can you deduce $a = 2$ from the hypotheses?

`Exercise 2`
Using $641 = 2^4 + 5^4 = 2^7 \cdot 5 + 1$, show that 641 divides the Fermat number $F_5 = 2^{32} + 1$.

`Exercise 3` (compare with exercise III.4 of Weil's book)
Let n be an integer > 1. Check that n can be written as the sum of (two or more) consecutive integers if and only if n is not a power of 2.

`Exercise 4` (exercise IV.3 of Weil's book)
Let a, m and n be positive integers with $m \neq n$. Check that the greatest common divisor (gcd) of $a^{2^m} + 1$ and $a^{2^n} + 1$ is 1 if a is even and 2 if a is odd. Deduce the existence of infinitely many primes.

`Exercise 5` (exercise IV.5 of Weil's book)
Check that the product of the divisors of an integer a is $a^{D/2}$ where D is the number of divisors of a.

`Exercise 6` (exercise V.7 of Weil's book)
Given $n > 0$, any $n + 1$ of the first $2n$ integers $1, \ldots, 2n$ contain a pair x, y such that y/x is a power of 2.

`Exercise 7` (exercise V.3 of Weil's book)
If n is a positive integer, then

$$2^{2n+1} \equiv 9n^2 - 3n + 2 \pmod{54}.$$

`Exercise 8` (exercise V.4 of Weil's book)
If x, y, z are integers such that $x^2 + y^2 = z^2$, then $xyz \equiv 0 \pmod{60}$.

`Exercise 9` (exercise VI.2 of Weil's book)
Solve the pair of congruences

$$5x - 7y \equiv 9 \pmod{12}, \quad 2x + 3y \equiv 10 \pmod{12};$$

show that the solution is unique modulo 12.

`Exercise 10` (exercise VI.3 of Weil's book)
Solve $x^2 + ax + b \equiv 0 \pmod{2}$

`Exercise 11` (exercise VI.4 of Weil's book)
Solve $x^2 - 3x + 3 \equiv 0 \pmod{7}$.

`Exercise 12` (exercise VI.5 of Weil's book)
The arithmetic mean of the integers in the range $[1, m-1]$ prime to m is $m/2$.

`Exercise 13` (exercise VI.6 of Weil's book)
When m is an odd positive integer,

$$1^m + 2^m + \cdots + (m-1)^m \equiv 0 \pmod{m}.$$

`Exercise 14` (exercise VIII.3 of Weil's book)
If p is an odd prime divisor of $a^{2^n}+1$ with $n \geq 1$, show that $p \equiv 1 \pmod{2^{n+1}}$.

`Exercise 15` (exercise VIII.4 of Weil's book)
If a and b are positive integers and $a = 2^\alpha 5^\beta m$ with m prime to 10, then the decimal expansion for b/a has a period ℓ where the number of decimal digits of ℓ divides $\varphi(m)$. Further, if there is no period with less than $m-1$ digits, then m is prime.

`Exercise 16` (exercise X.3 of Weil's book)
For p prime and n positive integer,

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } p-1 \text{ does not divide } n, \\ -1 \pmod{p} & \text{if } p-1 \text{ divides } n. \end{cases}$$

http://www.math.jussieu.fr/~miw/

SEAMS School 2013 ITB
Number theory (solutions)

Solution of Exercise 1. From

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1),$$

it follows that $a-1$ divides $a^n - 1$. Since $a \geq 2$ and $n \geq 2$, the divisor $a-1$ of $a^n - 1$ is $< a^n - 1$. If $a^n - 1$ is prime then $a - 1 = 1$, hence $a = 2$.

If $n = bc$, then $a^n - 1$ is divisible by $a^c - 1$, as we see from the relation

$$x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + x^2 + x + 1)$$

with $x = a^c$. Hence if $2^n - 1$ is prime, then n is prime.

If n has an odd divisor $d > 1$, then the identity

$$b^d + 1 = (b+1)(b^{d-1} - b^{d-2} + \cdots + b^2 - b + 1)$$

with $b = a^{n/d}$ shows that $b+1$ divides $a^n + 1$. Hence if $a^n + 1$ is prime, then n has no odd divisor > 1, which means that n is a power of 2. Also $a^n + 1$ is odd, hence a is even.

It may happen that $a^n + 1$ is prime with $a > 2$ – for instance when a is a power of 2 (Fermat primes), but also for other even values of a like $a = 6$ and $n = 2$. It is a famous open problem to prove that there are infinitely many integers a such that $a^2 + 1$ is prime.

□

Solution of Exercise 2. Write

$$641 = 2^4 + 5^4 = 2^7 \cdot 5 + 1,$$

so that on the one hand

$$5 \cdot 2^7 \equiv -1 \pmod{641},$$

hence

$$5^4 2^{28} \equiv (-1)^4 \equiv 1 \pmod{641},$$

and on the other hand

$$5^4 \cdot 2^{28} \equiv -2^{32} \pmod{641}.$$

Hence

$$2^{32} \equiv -1 \pmod{641}.$$

`Remark`. One can repeat the same proof without using congruences. From the identity

$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

we deduce that for any integer x, the number $x^4 - 1$ is divisible by $x+1$. Take $x = 5 \cdot 2^7$; it follows that $x + 1 = 641$ divides $5^4 2^{28} - 1$. However 641 also divides $2^{28}(2^4 + 5^4) = 2^{32} + 5^4 2^{28}$, hence 641 divides the difference

$$(2^{32} + 5^4 2^{28}) - (5^4 2^{28} - 1) = 2^{32} + 1 = F_5.$$

□

Solution of Exercise 3. Assume first that $n \geq 3$ is not a power of 2. Let $2a+1$ be an odd divisor of n with $a \geq 1$. Write $n = (2a+1)b$.

If $b > a$ then n is the sum

$$(b-a) + (b-a+1) + \cdots + (b-1) + b + (b+1) + \cdots + (b+a)$$

of the $2a+1$ consecutive integers starting with $b-a$.

If $b \leq a$ then n is the sum

$$(a-b+1) + (a-b+2) + \cdots + \cdots + (a+b)$$

of the $2b$ consecutive integers starting with $a-b+1$.

Assume now n is a sum of b consecutive integers with $b > 1$:

$$n = a + (a+1) + \cdots + (a+b-1) = ba + \frac{b(b+1)}{2}\cdot$$

Then

$$2n = b(2a+b+1)$$

is a product of two numbers with different parity, hence $2n$ has an odd divisor and therefore n is not a power of 2. □

Solution of Exercise 4. Without loss of generality we assume $n > m$. Define $x = a^{2^m}$, and notice that

$$a^{2^n} - 1 = x^{2^{n-m}} - 1$$

which is divisible by $x + 1$. Hence $a^{2^m} + 1$ divides $a^{2^n} - 1$. Therefore if a positive integer d divides both $a^{2^m}+1$ and $a^{2^n}+1$, then it divides both $a^{2^n}-1$ and $a^{2^n} + 1$, and therefore it divides the difference which is 2. Hence $d = 1$ or 2. Further, $a^{2^n} + 1$ is even if and only if a is odd.

For $n \geq 1$, let P_n be the set of prime divisors of $2^{2^n}+1$. The set P_n is not empty, and the sets P_n for $n \geq 1$ are pairwise disjoint. Hence their union is infinite. □

Solution of Exercise 5. A one line proof:

$$\left(\prod_{d|a} d\right)^2 = \left(\prod_{d|a} d\right)\left(\prod_{d|a} \frac{a}{d}\right) = \left(\prod_{d|a} a\right) = a^D.$$

`Remark.` A side result is that if a is not a square, then D is even.

□

Solution of Exercise 6. Let $x_1, \ldots, x_{n+1}$ be $n + 1$ distinct positive integers $\leq 2n$. For $i = 1, \ldots, n+1$, denote by y_i the largest odd divisor of x_i. Notice that $1 \leq y_i \leq n$ for $1 \leq i \leq n + 1$. By Dirichlet box principle, there exist $i \neq j$ such that $y_i = y_j$. Then x_i and x_j have the same largest odd divisor, which means that x_i/x_j is a power of 2.

□

Solution of Exercise 7. For $n = 0$ both sides are equal to 2, for $n = 1$ to 8. We prove the result by induction. Assume

$$2^{2n-1} \equiv 9(n-1)^2 - 3(n-1) + 2 \pmod{54}.$$

The right hand side is $9n^2 - 21n + 14$, and

$$4(9n^2 - 21n + 14) = 36n^2 - 84n + 56$$

which is congruent to $9n^2 - 3n + 2$, since $27n(n + 3)$ is a multiple of 54.

□

Solution of Exercise 8. Since $60 = 2^2 \cdot 3 \cdot 5$, we just need to check that 4, 3 and 5 divide xyz.

If two at least of the numbers x, y, z are even, then 4 divides xyz. If only one of them, say t, is even, then t^2 is either the sum or the difference of two odd squares. Any square is congruent to 0, 1 or 4 modulo 8. Hence $t^2 \equiv 0 \pmod 8$, which implies $t \equiv 0 \pmod 4$. Therefore $xyz \equiv 0 \pmod 4$.

The squares modulo 3 are 0 and 1, hence z^2 is not congruent to 2 modulo 3, and therefore x^2 and y^2 are not both congruent to 1 modulo 3: one at least of them is 0 modulo 3, hence 3 divides xy.

Since the squares modulo 3 are 0 and 1, the same argument shows that 5 divides xy.

□

Solution of Exercise 9. Multiply the first equation by 3, the second by 7 and add. From $29 \equiv 5 \pmod{12}$ and $97 \equiv 1 \pmod{12}$ we get $5x \equiv 1 \pmod{12}$. Since

$$5 \times 5 - 2 \times 12 = 1,$$

the inverse of 5 modulo 12 is 5. Hence $x \equiv 5 \pmod{12}$. Substituting yields $y \equiv 4 \pmod{12}$.

The unicity can also be proved using the fact that the determinant of the system

$$\begin{vmatrix} 5 & -7 \\ 2 & 3 \end{vmatrix}$$

is 29 which is prime to 12.

□

Solution of Exercise 10. (Compare with exercise XI.2: *If p is an* odd *prime and a is prime to p, show that the congruence $ax^2 + bx + c \equiv 0 \pmod p$ has two solutions, one or none according as $b^2 - 4ac$ is a quadratic residue,* 0 *or a non–residue modulo p*).

If a is even, the discriminant in $\mathbf{F}_2$ is 0, and there is a unique solution $x \equiv b \pmod 2$.

If a is odd, the discriminant is not 0 (hence it is 1 in $\mathbf{F}_2$). If b is even there are two solutions (any $x \in \mathbf{F}_2$ is a solution, $x(x+1)$ is always even), if b is odd there is no solution: $x^2 + x + 1$ is irreducible over $\mathbf{F}_2$.

□

Solution of Exercise 11. In the ring $\mathbf{F}_7[X]$ of polynomials over the finite field $\mathbf{Z}/7\mathbf{Z} = \mathbf{F}_7$, we have

$$X^2 - 3X + 3 = (X+2)^2 - 1 = (X+1)(X+3).$$

The roots of this polynomial are

$$x = 6 \pmod 7 \quad \text{and} \quad x = 4 \pmod 7.$$

$\square$

Solution of Exercise 12. We define a partition of the set of integers k in the range $[1, m-1]$ prime to m into two or three subsets, where one subset consists of those integers k which are $< m/2$, another subset consists of those integers k which are $> m/2$, with an extra third set with a single element $\{m/2\}$ if m is congruent to 2 modulo 4. The result follows from the existence of a bijective map $k \mapsto m - k$ from the first subset to the second.

$\square$

Solution of Exercise 13. Use the same argument as in Exercise 12 with

$$k^m + (m-k)^m \equiv 0 \pmod m \quad \text{for} \quad 1 \le k \le m$$

since m is odd.

$\square$

Solution of Exercise 14. The property that p divides $a^{2^n} + 1$ is equivalent to $a^{2^n} \equiv -1 \pmod p$, which means also that a has order 2^{n+1} modulo p. Hence in this case 2^{n+1} divides $p - 1$.

For $n = 5$, this shows that any prime divisor of $2^{2^5} + 1$ is congruent to 1 modulo $2^6 = 64$. It turns out that 641 divides the Fermat number F_5 (see exercise 2). $\square$

Solution of Exercise 15. For c a positive integer, the decimal expansion of the number

$$\frac{1}{10^c - 1} = 10^{-c} + 10^{-2c} + \cdots$$

is periodic, with a period having c decimal digits, namely $c-1$ zeros followed by one 1. For $1 \le r < 10^c - 1$, the number

$$\frac{r}{10^c - 1}$$

has a periodic decimal expansion, with a period (maybe not the least one) having c decimal digits, these digits are the decimal digits of r. Adding a positive integer to a real number does not change the expansion after the decimal point. The decimal expansion of the product of a real number x by a power of 10 is obtained by shifting the decimal expansion of x (on the right or on the left depending of whether it is a positive or a negative power of 10).

We claim that a number of the form

$$\frac{k}{10^\ell(10^c-1)},$$

where k, ℓ and c are integers with $k>0$ and $c>0$, has a decimal expansion which is ultimately periodic with a period of length c. Indeed, using the Euclidean division of k by 10^c-1, we write

$$k=(10^c-1)q+r \quad \text{with} \quad 0\le r<10^c-1,$$

hence

$$\frac{k}{10^\ell(10^c-1)}=\frac{1}{10^\ell}\left(q+\frac{r}{10^c-1}\right),$$

and our claim follows from the previous remarks.

Now we consider the decimal expansion of b/a when a and b are positive integers and $a=2^\alpha 5^\beta m$ with m prime to 10. Denote by c the order of the class of 10 modulo m. Then c divides $\varphi(m)$, $10^c\equiv 1 \pmod m$ and

$$\frac{b}{a}10^{\alpha+\beta}(10^c-1)\in\mathbf{Z}.$$

Therefore b/a has a decimal expansion with a period having c decimal digits. If c is the smallest period and if $c=m-1$, then $m-1$ divides $\varphi(m)$, hence $\varphi(m)=m-1$ and m is prime. For instance with $a=m=7$, $\alpha=\beta=0$, $b=1$:

$$1/7=0.142857\,142857\,142857\,14\dots$$

has minimal period of length 6.

$\square$

Solution of Exercise 16. If $p-1$ divides n, then $a^n\equiv 1 \pmod p$ for $a=1,\dots,p-1$, the sum has $p-1$ terms all congruent to 1 modulo p, hence the sum is congruent to -1 modulo p.

Assume $p-1$ does not divide n. Let ζ be a generator of the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$. Since ζ has order $p-1$, the condition that $p-1$ does not divide n means $\zeta^n \neq 1$. Let $d = \gcd(p-1, n)$ and $q = (p-1)/d$.

We claim that the order of ζ^n is q. Indeed, we can write $n = d\delta$. Since ζ has order $p-1$ it follows that ζ^d has order q, and since $\gcd(\delta, q) = 1$, $\zeta^n = (\zeta^d)^\delta$ has also order q.

Therefore the sequence $(1^n, 2^n, \ldots, (p-1)^n)$, which is a permutation of the sequence $(1, \zeta^n, \zeta^{2n}, \ldots, \zeta^{(p-2)n})$, is a repetition d times of the sequence $(1, \zeta^n, \zeta^{2n}, \ldots, \zeta^{(q-1)n})$. Also $(\zeta^n)^q = 1$. Hence

$$1^n + 2^n + \cdots + (p-1)^n = \sum_{j=0}^{p-2} \zeta^{jn} = d \sum_{j=0}^{q-1} \zeta^{jn} = \frac{(\zeta^n)^q - 1}{\zeta^n - 1} = 0.$$

□

References

[1] WEIL, ANDRÉ. – *Number theory for beginners.* With the collaboration of Maxwell Rosenlicht. Springer-Verlag, New York-Heidelberg, 1979.
MR 80e:10004
http://link.springer.com/book/10.1007%2F978-1-4612-9957-8

http://www.math.jussieu.fr/~miw/