AUF (Agence Universitaire pour la Francophonie) September/october 2005
Coopération Mathématique inter-universitaire Cambodge France *Michel Waldschmidt*

Master Training Program : Royal Academy of Cambodia/CIMPA

Written control: `october 21, 2005`

Timing: 3 hours
No document, no calculator

All answers require a proof.

1.
a) Does there exist three sets E, F, G and two maps

$$f : E \to F, \qquad g : F \to G$$

such that f is not injective, g is not surjective and at the same time $g \circ f : E \to G$ is bijective?
b) Does there exist three sets E, F, G and two maps

$$f : E \to F, \qquad g : F \to G$$

such that f is not surjective, g is not injective and at the same time $g \circ f : E \to G$ is bijective?
For each of these two questions, if your answer is no, prove it. If your answer is yes, give an example.

2. For each of the three following numbers (in decimal notation), say whether it is rational, if so give its irreducible form a/b with a and b relatively prime and $b > 0$:

$$0.123123123123123\ldots,$$
$$0.1999999999999\ldots$$
$$0.10100100010000100000100000010000000 1\ldots,$$

`Hint:` in the last example the sequences of consecutive 0 have successively 1, 2, 3, 4, ... terms.

3. How many divisors has the number 86 400 000 ?

4. Among the integers n in the range $1 \leq n \leq 10\,000$, how many
a) are relatively prime to 10 000?
b) are relatively prime to 21?

5.
a) What is the value of the gcd (greatest common divisor) d_1 of the two numbers 2^{360} and 2^{240} ?
b) What is the value of the gcd d_2 of the two numbers $2^{360}-1$ and $2^{240}-1$?
c) What is the value of the gcd d_3 of the two numbers $2^{360}-1$ and 2^{240} ?
d) For each of these three numbers d_1, d_2, d_3,
– how many binary digits (= in basis 2) has-it?
– approximately how many decimal digits has-it? Use the fact that the number $2^{10}=1024$ is not far from 10^3.
– what is the last decimal digit?.

6. For each of the following four prime numbers 37, 41, 43, 47, say
– whether 1 is a quadratic residue or not,
– whether -1 is a quadratic residue or not,
– whether 2 is a quadratic residue or not,
– whether -2 is a quadratic residue or not,
– whether 3 is a quadratic residue or not,
– whether 4 is a quadratic residue or not.

7. We consider a finite field with 64 elements.
a) What is the characteristic of this field?
b) Which are the integers $n \geq 1$ for which there exists at least one primitive n-th root of unity in this field?
For each of these values of n, how many primitive n-th roots of unity are they in this field?

8. Which are the generators of the cyclic group $(\mathbf{Z}/7\mathbf{Z})^\times$?
Which are the prime numbers p such that the cyclotomic polynomial $\Phi_7(X)$ is irreductible over the finite field $\mathbf{F}_p$ with p elements?

9. Let $f \in \mathbf{F}_p[X]$ be an irreducible polynomial of degree d over the finite field $\mathbf{F}_p$ with p elements, K a finite field of characteristic p and $\alpha \in K$ a root of f. Give the list of roots of f in K.

10. Give the list of elements in the cyclic code of length 7 over $\mathbf{F}_2$ whose generating polynomial is $1+X+X^2+X^3+X^4+X^5+X^6$.

11. Let n be an integer ≥ 2. Denote by F_n the Fermat number $2^{2^n}+1$. Let p be a prime divisor of F_n.
a) What is the order of 2 modulo p ?
b) Deduce that p is congruent to 1 modulo 2^{n+1}.
c) Is 2 a quadractic residue modulo p ?
d) Show that p is congruent to 1 modulo 2^{n+2}.

`The solution will soon be available on the web site`
http://www.math.jussieu.fr/∼miw/enseignement.html