Solutions to exam paper 3701, 2007/2008

1(a) Show that there are arbitrarily large gaps between consecutive primes.

Answer: Let $n \in \mathbb{N}$, we show that none of the following consecutive n numbers are prime:

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1).$$

Indeed, the number $(n+1)!+k$ is divisible by k for each $k = 2, 3, \ldots, (n+1)$.

1(b) Suppose $k, n \in \mathbb{N}$ and $k \geq 2$. Show that if $\sqrt[k]{n}$ is rational, then n is the kth power of an integer.

Answer: Suppose $\sqrt[k]{n}$ is a rational number, say b/c with $b, c \in \mathbb{N}$. Then $n \cdot c^k = b^k$. Let $n = \prod p^{\alpha(p)}$, $b = \prod p^{\beta(p)}$, $c = \prod p^{\gamma(p)}$ be the canonical representations. The exponents of p on the two sides of the equation $n \cdot c^k = b^k$ have to be equal, that is $\alpha(p) + k\gamma(p) = k\beta(p)$. Then $0 \leq \alpha(p) = k(\beta(p) - \gamma(p))$ showing that $\beta(p) \geq \gamma(p)$ for every p. This implies, in turn, that $r = b/c$ is an integer, and then n is the kth power of r.

1(c) What is the input and the output of the squaring and reducing algorithm? What is the size of the input? Give an upper bound, as a function of the size of the input, on the number of iterations this algorithm can take. Determine the last two digits of 11^{201}.

Answer: The input is $a, k, m \in \mathbb{N}$, and the output is an integer b with $0 \leq b < m$ and $b \equiv a^k \bmod m$. The size of the input is the sum of the sizes, that is, number of decimal digits, of a and k and m. The squaring and reducing algorithm takes at most as many iterations as the number of binary digits, say s, of k. Then $2^{s-1} \leq k < 2^s$. It follows that $(s-1)\log_{10} 2 \leq \log_{10} k < K$ where K is the size of k. Thus the number of iterations is at most $1 + K/\log_{10} 2 < 5K$. For computing the last two digits of 11^{201} we use squaring and reducing mod 100. The binary representation of 201 is $100\underline{10011}_2$. The sequence of reduced squares is $11, 21, 41, 81, 61, 21, 41, 81$, and so $11^{201} = 11 \cdot 81 \cdot 41 \cdot 81 = 11 \bmod 100$.

2(a) Give the definition of a reduced residue system mod m. Show that if $(a, m) = 1$ and $r_1, \ldots, r_s$ is a reduced residue system mod m, then so is $ar_1, \ldots, ar_s$.

Answer: Integers $r_1, \ldots, r_s$ form a reduced residue system mod m by definition, if $(r_i, m) = 1$ for every i and if for every $z \in \mathbb{Z}$ with $(z, m) = 1$ there is a unique r_i congruent to z. In other words, every residue class which is relatively prime to m is represented uniquely by some r_i. To prove the statement one should check two things: (1) $(ar_i, m) = 1$ for every r_i, and (2) $ar_i \equiv ar_j \bmod m$ implies $i = j$. As for (1), a and m have no common prime divisor, and r_i and m have no common prime divisors. By the fundamental theorem of arithmetic the prime divisors of ar_i are exactly the prime divisors of a and r_i, and so ar_i and m have no common prime divisor either, implying $(ar_i, m) = 1$. For (2) note that, since $(a, m) = 1$, the congruence $ar_i \equiv ar_j \bmod m$ can be simplified by a yielding $r_i \equiv r_j \bmod m$. This implies, by definition, that $r_i = r_j$.

2(b) State and prove Wilson's theorem.

Answer: Wilson's theorem. If $p \in \mathbb{P}$, then $(p-1)! \equiv -1 \bmod p$. For the proof we use the fact that every $a \in \mathbb{Z}$ with $(a, m) = 1$ has an inverse $\overline{a}$ which is unique mod m, and that the inverse of the inverse is the number itself. Now in the product $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ every number has an inverse (since $p \in \mathbb{P}$). We pair up every number with its inverse. Such a pair is (a, a) and their product is just $1 \bmod p$ by the definition of the inverse. This works unless $a \equiv \overline{a} \bmod p$, in this case, however $a^2 \equiv 1 \bmod p$. Then $p | a^2 - 1 = (a-1)(a+1)$ and so $a \equiv 1$ or $a \equiv -1 \bmod p$. So only 1 and $p-1$ cannot be paired up with their inverses. This gives $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \bmod p$ indeed.

2(c) Assume p is a prime. Show that there are integers a, b such that $a^2 + b^2 \equiv 2 \bmod p$.

Answer: Assume p is odd, and define $\overline{p} = (p-1)/2$. (The case $p = 2$ is very simple.) The set $T_1 = \{0, 1^2, 2^2, \ldots, \overline{p}^2\}$ consists of $\overline{p} + 1$ numbers, every two of them distinct mod p. The same holds for $T_2 = \{2, 2 - 1^2, 2 - 2^2, \ldots, 2 - \overline{p}^2\}$. By the pigeonhole principle there are numbers a and b with $a^2 \in T_1$ and $2 - b^2 \in T_2$ such that $a^2 \equiv 2 - b^2 \bmod p$. This is the same as $a^2 + b^2 \equiv 2 \bmod p$. Alternatively, $a = 1, b = 1$ gives $a^2 + b^2 \equiv 2 \bmod p$.

3(a) Define the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$. Using the fact that $\sum_{d|n} \mu(d) = 0$ for all $n \geq 2$, $n \in \mathbb{N}$, prove that $(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2})(\sum_{k=1}^{\infty} \frac{1}{k^2}) = 1$.

Answer: Definition: $\mu(n) = 0$ if $n \in \mathbb{N}$ is not squarefree, if n is squarefree, then it is the product of s distinct primes and $\mu(n) = (-1)^s$.

In the product of the two sums we have to add the terms $\mu(d)/(d^2k^2)$ for all pairs $(d, k) \in \mathbb{N} \times \mathbb{N}$. Substituting $n = dk$, this is the same as adding all terms $\mu(d)/n^2$ for all $n, d \in \mathbb{N}$ with $d|n$:

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \cdot \sum_{k=1}^{\infty} \frac{1}{k^2} = \sum_{n=1}^{\infty} \sum_{d|n} \frac{\mu(d)}{n^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{d|n} \mu(d) = 1,$$

as $\sum_{d|n} \mu(d) = 0$ unless $n = 1$ by a theorem from class.

3(b) Let $f(x)$ be a polynomial with integral coefficients. Define the degree of the congruence $f(x) \equiv 0 \bmod m$. Show that if p is a prime, then $f(x) \equiv 0 \bmod p$ cannot have more solutions mod p than its congruence degree.

Answer: Letting $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0$, the degree of the congruence $f(x) \equiv 0 \bmod m$ is the largest j such that a_j is not divisible by m. The congruence degree is undefined if all a_j are divisible by m. Let n be the congruence degree of $f(x) \equiv 0 \bmod p$. We prove the statement by induction on n. For $n = 0$, $f(x) \equiv a_0 \bmod p$ where a_0 is not congruent to 0, with no solution whatsoever. For $n = 1$, $f(x) \equiv a_1 x + a_0$ with a_1 not congruent to $0 \bmod p$, which has the unique solution $-a_0\overline{a_1} \bmod p$ where $\overline{a_1}$ is the inverse of $a_1 \bmod p$. For the induction step from $n-1$ to n (where $n \geq 2$) there is nothing to prove if our congruence has at most one solution. So let b be a solution to $f(x) \equiv 0 \bmod p$. Then $f(x) \equiv f(x) - f(b) = \sum a_n(x^n - b^n) + \ldots + a_1(x-b) \equiv (x-b)g(x) \bmod p$, where $g(x)$ is a polynomial with integral coefficients. This follows from the fact that $x^k - b^k = (x - b)(x^{k-1} + x^{k-2} + \ldots + b^{k-1})$. Then every solution to $f(x) \equiv 0 \bmod p$, distinct from b, is a solution to $g(x) \equiv 0 \bmod p$. It is clear that the congruence degree of $g(x) \equiv 0 \bmod p$ is exactly $n - 1$. By the induction hypothesis, it has at most $n - 1$ solutions. Then $f(x) \equiv 0 \bmod p$ has at most $1 + (n - 1) = n$ solutions.

3(c) Let Q denote the set of integers that can be written as sum of two squares. Assume $n \in \mathbb{N}$. Does $n \equiv 1 \bmod 4$ imply that $n \in Q$? Does $n \equiv -1 \bmod 4$ imply that $n \notin Q$?

Answer: The example $n = 21$ shows, via the characterization theorem for Q, that $n \equiv 1 \bmod 4$ does not imply that $n \in Q$. On the other hand, $n \equiv -1 \bmod 4$ implies that $n \notin Q$. Indeed, assuming $n \in Q$, all prime factors $q \equiv -1 \bmod 4$ of n have even exponent (by the characterization theorem for Q). Consequently $n \equiv 1 \bmod 4$.

4(a) Define the Legendre symbol $\left(\frac{a}{p}\right)$. Show that the congruence $x^2 \equiv 3 \bmod 47$ has two solutions. Can you find these solutions explicitly?

Answer: Assuming $p \in \mathbb{P}$ and $a \in \mathbb{Z}$, the Legendre symbol $\left(\frac{a}{p}\right)$ equals 0 if $p|a$, equals 1 if a is a quadratic residue $\bmod p$ and equals -1 if a is a quadratic non-residue $\bmod p$. For computing we use quadratic reciprocity: $\left(\frac{3}{47}\right) = -\left(\frac{47}{3}\right) = -\left(\frac{2}{3}\right) = 1$. The solutions can be found explicitly using a theorem from class saying that if $p \in \mathbb{P}$ with $p \equiv 3 \bmod 4$, $(a,p) = 1$ and $x^2 \equiv a \bmod p$ has a solution, then the solutions are exactly $\pm a^{(p+1)/4} \bmod p$. Now $3^{12} \equiv 12 \bmod 47$, so the solutions are $x = \pm 12$.

4(b) Give the definition of the order of $a \bmod m$. Show that $a^k \equiv 1 \bmod m$ if and only if k is a multiple of the order of $a \bmod m$. What is the order of 3 and 5 $\bmod 23$?

Answer: Assuming $a, m \in \mathbb{N}$ and $(a,m) = 1$ the order of $a \bmod m$ is, by definition, the smallest positive integer h with $a^h \equiv 1 \bmod m$. Suppose h is the order of $a \bmod m$. If $h|k$, that is $k = th$ for some integer t, then $a^k = a^{th} = (a^h)^t \equiv 1^t = 1 \bmod m$. On the other hand, if $a^k \equiv 1 \bmod m$ for some $k \in \mathbb{N}$, then by division with remainder $k = th + r$ with $t, r \in \mathbb{Z}$ and $0 \leq r < h$. This implies $a^k = a^{th+r} \equiv a^r \equiv 1 \bmod m$ which is possible only when $r = 0$. Thus indeed $h|k$. The order of 3 $\bmod 23$ is 11, and the order of 5 $\bmod 23$ is 22.

4(c) State and prove the theorem on the number of solutions to the congruence $x^n \equiv a \bmod p$ where $a, n, p \in \mathbb{N}$, p is a prime and $(a,p) = 1$.

Answer: Theorem: Define $d = (n, p-1)$. Under the above conditions the congruence $x^n \equiv a \bmod p$ has d solutions if $a^{(p-1)/d} \equiv 1 \bmod p$ and has no solution otherwise.

For the proof let g be a primitive root $\bmod p$. Then $a = g^\alpha$ with a unique $\alpha \bmod p-1$. We seek the solution in the form $x = g^z$. Then the original congruence is equivalent to $g^{nz} \equiv g^\alpha \bmod p$. By a theorem from class this is equivalent to $nz \equiv \alpha \bmod p-1$. This is a linear congruence in one variable, which has d solutions if $d|\alpha$ and no solution otherwise. Now $a^{(p-1)/d} = g^{\alpha(p-1)/d}$ is congruent to 1 $\bmod p$ iff the exponent is a multiple of $p-1$ by the properties of the primitive root. Clearly, $\alpha(p-1)/d$ is a multiple of $p-1$ iff α/d is an integer, that is, iff $d|\alpha$.

5(a) Solve the congruence $x^3 - x^2 \equiv 4 \bmod 7^3$.

Answer: We check by hand that $x^3 - x^2 \equiv 4 \bmod 7$ has exactly two solutions: 2 and 3. We try to lift these solutions by Hensel's lemma. Set $f(x) = x^3 - x^2 - 4$. Then $f'(x) = 3x^2 - 2x$, so $f'(2) \equiv 1 \bmod 7$. This solution lifts to a unique solution $2 - \overline{f'(2)}f(2) \equiv 2 \bmod 7^2$ since $f(2) = 0$. This solutions lifts further to the uniques solution $x = 2 \bmod 7^3$. Next $f'(3) \equiv 0 \bmod 7$ and $f(3) = 14$ which is non zero mod 7^2, so this solution does not lift any further. The original congruence has a unique solution, $x \equiv 2 \bmod 7^3$.

5(b) State the key lemma to the RSA public key cryptosystem. Explain how authentification works.

Answer: Key lemma. Assume $a, k, m \in \mathbb{N}$ with $(a, m) = 1$, $(k, \Phi(m)) = 1$, and let $\overline{k}$ be the inverse of $k \bmod \Phi(m)$. Then $a^{k\overline{k}} \equiv a \bmod m$. Further, if $r_1, \ldots r_s$ is a reduced residue system mod m, then so is $r_1^k, \ldots, r_s^k$.

In the RSA public key cryptosystem, everybody chooses two 100 digit primes, p and q, computes $m = pq$, and chooses a number k which is relatively prime to $\Phi(m) = (p-1)(q-1)$. Then $p, q, \Phi(m)$ and $\overline{k}$ are kept secret, while m and k are made public. Assume now that Sender wants to send a message a (a 200 digit number) to Receiver. Let m_S, k_S and m_R, k_R resp. be the public key of Sender and Receiver. Sender computes $b \equiv a^{\overline{k}_S} \bmod m_S$ (a 200 digit number), then computes $c \equiv b^{k_R} \bmod m_R$ (another 200 digit number), and makes the public statement "c is my message for Receiver". Receiver computes first $b \equiv c^{\overline{k}_R} \bmod m_R$, and then determines $a \equiv b^{k_S} \bmod m_S$. Authentification is guaranteed by the fact that only Sender can determine $a^{\overline{k}_S}$. Some caution is needed however when b (which is computed a number mod m_R) is considered by Receiver as a number mod m_S. But only at most ten 200 digit numbers are congruent to $b \bmod m_R$. One of them works, or the original message is not authentic.

5(c) State Dirichlet's theorem on Diophantine approximation. Find the value of the infinite continued fraction $[0; 1, 2, 1, 2, 1, 2, \ldots] = [0; \overline{1, 2}]$.

Answer: Theorem. For every $x \in \mathbb{R}$ and every $Q \in \mathbb{N}$ there are integers $p, q \in \mathbb{Z}$ with $1 \leq q \leq Q$ such that $|qx - p| < \frac{1}{(Q+1)}$.

Let x be the value $[0; \overline{1, 2}]$, then $x = [0; 1, 2, x]$. This gives the quadratic equation $x^2 + 2x - 2 = 0$ whose unique positive solution is $x = \sqrt{3} - 1$.