Please submit your solutions in class.

Please show all working.

1. Calculate the Legendre symbol $\left(\frac{1234}{89}\right)$.

Solution: $\left(\frac{1234}{89}\right) = \left(\frac{77}{89}\right) = \left(\frac{7}{89}\right)\left(\frac{11}{89}\right) = \left(\frac{5}{7}\right)\left(\frac{1}{11}\right) = \left(\frac{2}{5}\right) = -1.$

2. (a) Use Euler's criterion to check whether 7 is a quadratic residue modulo 23.

(b) Use Gauss's Lemma to check whether 7 is a quadratic residue modulo 23.

(c) Use quadratic reciprocity to calculate $\left(\frac{7}{23}\right)$.

Solution:

(a) $7^{11} \equiv (7^2)^5 \cdot 7 = 3^5 \cdot 7 = 4 \cdot 9 \cdot 7 = -1 \mod 23.$

(b)

x	1	2	3	4	5	6	7	8	9	10	11
$7x$	7	−9	−2	5	−11	−4	3	10	−6	1	8

There are 5 minus signs, hence $\left(\frac{7}{23}\right) = (-1)^5$.

(c) $\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1$ (since $7 \equiv -1 \mod 8$).

3. For which odd primes p is 7 a quadratic residue mod p.

Solution: $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$ if $p \equiv 1 \mod 4$.

$\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$ if $p \equiv 3 \mod 4$.

Now use the Chinese Remainder Theorem to solve the six systems

$p \equiv 1 \mod 4$ and $p \equiv 1, 2, 4 \mod 7$; and

$p \equiv -1 \mod 4$ and $p \equiv 3, 5, 6 \mod 7$.

Result: $p \equiv \pm 1, \pm 3, \pm 9 \mod 28$.

4. Find the square roots of 7 modulo 513.

Solution: Factorize: $513 = 3^3 \cdot 19$.

Solve the congruences $x^2 \equiv 7 \mod 3^3$ and $x^2 \equiv 7 \mod 19$. The solutions are $x \equiv \pm 13 \mod 27$ and $x \equiv \pm 8 \mod 19$, respectively.

Use CRT to get $x \equiv 68, 122, 391, 445 \mod 513$.

5. (a) Show that for an odd prime p there are as many square residue classes modulo p^e as non-square residue classes in $U(\mathbb{Z}_{p^e})$, $p \geq 1$.

(b) How many squares and how many non-squares are there in $U(\mathbb{Z}_{2^e})$?

Solution:

(a) $U(\mathbb{Z}_{p^e})$ is cyclic of (even) order $p^e - p^{e-1}$: $U(\mathbb{Z}_{p^e}) = \langle g \rangle$. The even powers of g form a subgroup of order $1/2(p-1)p^{e-1}$; the remaining $1/2(p-1)p^{e-1}$ elements are non-squares.
(The question should have asked about 'square residue classes modulo p^e, corrected above.)

(b) If $e \geq 3$, then $U(\mathbb{Z}_{2^e})$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{e-2}}$. Squares correspond to elements $(a,b)+(a,b) = (0,2b)$, i.e. there are as many squares as there are even numbers in $\mathbb{Z}_{2^{e-2}}$, i.e. a quarter of all elements of $U(\mathbb{Z}_{2^e})$ are squares, the remaining three quarters are non-squares.
$U(\mathbb{Z}_2)$ contains only one element which is a square, and $U(\mathbb{Z}_4) = \{1, -1\}$ contains one square and one non-square.

6. Let $p > 3$ be a prime. Prove that the product of all primitive roots mod p is congruent to 1 modulo p.

Solution: If r is a primitive root mod p then r^{-1} ia also a primitive root. In the product of all primitive roots, we therefore pair up pairs of inverses, giving the desired result. Could it happen that one of these roots does not find a partner (i.e. that it would be its own inverse)? No, because the order of a primitive root is $p - 1 \neq 2$.

7. (a) Prove that 2 is irreducible in the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-5})$.

(b) Prove that $1 + \sqrt{-5}$ is irreducible in the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-5})$.

Solution:

(a) If $2 = uv$, look at norms: $N(2) = N(u)N(v)$. If u, v are not units, then $N(u) \neq 1 \neq N(v)$. But $N(2) = 4$ and thus $N(u) = N(v) = 2$. But if $u = a + b\sqrt{-5}$, we have $N(u) = a^2 + 5b^2$, which is impossible for integers $a, b \in \mathbb{Z}$. (We have made use of the fact that integers in $\mathbb{Q}(\sqrt{-5})$ are of the form $a + b\sqrt{-5}$, where $a, b \in \mathbb{Z}$).

(b) Same as part (a).

8. Prove that for any $n \geq 3$ the numbers $\alpha_n = \cos(2\pi/n)$ are algebraic numbers but not algebraic integers. Determine the smallest b for which $b\alpha_n$ are algebraic integers for all $n \geq 3$.

Solution: If $\zeta_n = e^{2\pi i/n}$, then ζ_n and $\overline{\zeta_n} = \zeta^{-1}$ are roots of the polynomial $x^n - 1$, and therefore algebraic integers. Then $2\alpha_n = \zeta_n + \overline{\zeta_n}$ is also an algebraic integer.

In the case $n = 4$, it is clear that $\alpha_4 = 0$, and therefore this is an algebraic integer (question was put carelessly).

So, if $n \geq 3$ and $n \neq 4$, the smallest positive integer such that $b\alpha_n$ is an algebraic integer is $b = 2$. (Anticipating the result of the following discussion.)

To prove that α_n is not an algebraic integer for $n \neq 4$, we make use of the following fact: the primitive n-th roots of unity ($e^{2\pi ik/n}$ with $\gcd(k,n) = 1$) are roots of a monic irreducible polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ of degree $\phi(n)$ (Euler phi). If u is a primitive n-th root of 1, then clearly u^{-1} is also a primitive n-th root of unity, i.e. also a root of Φ_n, and therefore the polynomial $x^{-\phi(n)/2}\Phi_n(x)$ is a polynomial of degree $\phi(n)/2$ in $z = u + u^{-1}$, say $f_n(z)$, with integer coefficients. The roots of the polynomial f_n are the numbers $2\cos 2\pi k/n$ where $\gcd(n,k) = 1$. [So we have an explicit construction for the polynomial that shows that $2\alpha_n$ is an algebraic integer.]

We have $f_n(x) = (x - 2\alpha_n)(x - \beta_2)\cdots(x - \beta_{\phi(n)})$, where the β's are the remaining roots of f_n. The polynomial $g_n(x) = f_n(2x)$ has the numbers $\cos 2\pi k/n$ where $\gcd(n,k) = 1$ as roots, and after dividing by $2^{\phi(n)}$ we have a monic polynomial $q(x)$ with the same roots. And obviously, the constant term of q is not an integer, being nonzero (if $n \neq 4$) and of absolute value < 1 (product of cosines). Hence α_n is not an algebraic integer ($n \geq 3, n \neq 4$).