1. **Calendar code problem.** (20 points) Let $x$ be an integer and let $y = x^7$. Find the smallest positive integer $n$ such that $y^n \equiv x \pmod{2013}$ for all $x$.

**Solution:** This is a problem about the multiplicative group $(\mathbb{Z}/2013)^\times$, where we are looking for the inverse of the element 7. The structure of this group depends on the prime factorization of 2013. Since $2013 = 3 \cdot 11 \cdot 61$,

$$(\mathbb{Z}/2013)^\times = (\mathbb{Z}/3)^\times \times (\mathbb{Z}/11)^\times \times (\mathbb{Z}/61)^\times = C_2 \times C_{10} \times C_{60}.$$  

This means that we need $7n \equiv 1 \pmod{2, 10, 61}$ simultaneously. The first congruence is satisfied by any odd $n$, so write $n = 2m + 1$.

Next we need

\[
\begin{align*}
7(2m + 1) &= 14m + 7 \equiv 1 \pmod{10} \\
14m + 6 &= 0 \pmod{10} \\
7m + 3 &= 0 \pmod{5}
\end{align*}
\]

This is satisfied by $m \equiv 1 \pmod{5}$, so we write $m = 5k + 1$, and

\[
n = 2m + 1 = 2(5k + 1) + 1 = 10k + 3.
\]

Our third condition is

\[
\begin{align*}
7n &= 70k + 21 \equiv 1 \pmod{60} \\
70k + 20 &= 0 \pmod{60} \\
7k + 2 &= 0 \pmod{6}
\end{align*}
\]

This is satisfied by $k = 4$, giving $n = 10k + 3 = 43$.

2. Let $\zeta = e^{2\pi i/16} = \left(\sqrt{1+i}\right) / \sqrt{2}$ (a primitive 16th root of unity) and let $E = \mathbb{Q}(\zeta)$.

(a) (10 points) Find the minimal polynomial $f(x)$ of $\zeta$ and describe its zeros in terms of $\zeta$.

**Solution:** $\zeta$ is a zeros of

\[
x^{16} - 1 = (x + 1)(x - 1) = (x^8 + 1)(x^4 + 1)(x^2 + 1)(x + 1)(x - 1).
\]
Zeros of the latter factors are 8th roots, fourth roots and square roots of unity so \( \zeta \) is a zero of the first factor, namely an 8th root of \(-1\). The other zeros are the other primitive 16th roots of unity, which are the odd powers of \( \zeta \).

(b) (10 points) Find the Galois group \( G \) of \( E \) over \( \mathbb{Q} \) and describe its action on the roots of \( f(x) \). Denote by \( \alpha \) and \( \beta \) the automorphisms sending \( \zeta \) to \( \zeta^3 \) and \( \zeta^{-1} \) respectively.

**Solution:** We have

\[
\begin{align*}
\alpha^2(\zeta) &= \alpha(\zeta^3) = \zeta^9 \\
\alpha^4(\zeta) &= \alpha^2(\zeta^9) = \zeta^{81} = \zeta \\
\beta^2(\zeta) &= \beta(\zeta^{-1}) = \zeta,
\end{align*}
\]

so \( \alpha \) and \( \beta \) have orders 4 and 2. \( G \) is isomorphic to \( C_4 \times C_2 \). The action on the odd powers of \( \zeta \) is indicated in the following diagram.

\[
\begin{array}{cccccccc}
\zeta & \alpha & \beta & \zeta^9 & \alpha & \beta & \zeta^{11} & \alpha & \beta \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\zeta^3 & \alpha & \beta & \zeta^7 & \alpha & \beta & \zeta^5 & \alpha & \beta \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\zeta^5 & \alpha & \beta & \zeta^3 & \alpha & \beta & \zeta^9 & \alpha & \beta \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\zeta^9 & \alpha & \beta & \zeta^3 & \alpha & \beta & \zeta^9 & \alpha & \beta \\
\end{array}
\]

3. Let \( G \) be the Galois group of the previous problem.

(a) (10 points) Find all subgroups of order 4 in \( G \). Denote them by \( H_1, H_2 \) and so on.

**Solution:** The elements \( \alpha \) and \( \alpha \beta \) each generate a cyclic subgroup of order 4, which we will call \( H_1 \) and \( H_2 \) respectively. The subgroup \( H_3 \) generated by \( \alpha^2 \) and \( \beta \) is isomorphic to \( C_2 \times C_2 \).

(b) (20 points) Find the subfield \( K_i \) of \( E \) fixed by each \( H_i \).

**Solution:** In each case the field \( K_i \) is a quadratic extension of \( \mathbb{Q} \), since the subgroup has index 2. We find it by looking for an element fixed by \( H_i \) that is not in \( \mathbb{Q} \).

For \( H_1 = \langle \alpha \rangle \), the element \( x_1 = \zeta^2 + \zeta^6 \) will do. Then we have

\[
x_1^2 = \zeta^4 + 2\zeta^8 + \zeta^{12} = \zeta^4 - 2 - \zeta^4 = -2,
\]

so the field is \( K_1 = \mathbb{Q}(\sqrt{-2}) \).

For \( H_2 \), its generator \( \alpha \beta \) fixes \( \zeta^4 = i \), so the field is \( K_2 = \mathbb{Q}(\sqrt{-1}) \).
For $H_3$, the element $x_3 = \zeta^2 + \zeta^{-2}$ is fixed by both $\alpha^2$ and $\beta$. Then we have

$$x_3^2 = \zeta^4 + 2 + \zeta^{-4} = \zeta^4 + 2 - \zeta^4 = 2$$

so $K_3 = \mathbb{Q}(\sqrt{2})$.

4. Let $F = \mathbb{Q}(\sqrt{-3})$ and let $E$ be the splitting field over $F$ of $f(x) = x^6 - 5$.

(a) (10 points) Find the zeros of $f(x)$.

**Solution:** Since $f(x) = x^6 - 5$, its roots are the sixth roots of 5. Let $\zeta = e^{2\pi i/6} = (1 + \sqrt{-3})/2$. Then these roots are

$$\left\{\zeta^j \sqrt[6]{5} : 0 \leq j \leq 5\right\}$$

(b) (10 points) Find the Galois group $H$ of $E$ over $F$.

**Solution:** The field is $E = F(\sqrt[6]{5})$. There is a field automorphism $\rho$ over $F$ that multiplies each zero of $f(x)$ by $\zeta$. It has order 6 and the group is $C_6$.

(c) (10 points) Let $\alpha = \sqrt[6]{5}$, the positive real sixth root of 5, $1.30766\ldots$. There is a field automorphism $\phi$ of $E$ over $\mathbb{Q}$ with $\phi(\alpha) = \alpha$ and $\phi(\sqrt{-3}) = -\sqrt{-3}$. Describe its action on the zeros of $f(x)$. HINT: IT HELPS TO PICTURE THESE ZEROS AS THE VERTICES OF A HEXAGON.

**Solution:** We have

$$\phi(\zeta) = \phi\left(\frac{1 + \sqrt{-3}}{2}\right) = \frac{1 - \sqrt{-3}}{2} = \zeta^5 = \zeta^{-1}.$$ 

It follows that $\phi(\pm \alpha) = \pm \alpha$, $\phi(\pm \zeta \alpha) = \pm \zeta^{-1} \alpha$ and $\phi(\pm \zeta^2 \alpha) = \pm \zeta^{-2} \alpha$.

(d) (10 points) Find the Galois group $G$ of $E$ over $\mathbb{Q}$ by describing its action on the zeros of $f(x)$. Determine whether it is solvable or not, and prove your answer.

**Solution:** The field is $E = F(\alpha) = \mathbb{Q}(\alpha, \sqrt{-3})$. We have $[E : \mathbb{Q}] = [F : \mathbb{Q}] = 6 \cdot 2 - 12$. $G$ permutes the six zeros of $f(x)$, which are the vertices of a hexagon in the complex plane. The automorphism $\rho$ rotates them counterclockwise through an angle of $\pi/3$, and $\phi$ reflects through the $x$-axis. These generate the dihedral group $D_{12}$, the symmetry group of the hexagon.

$G$ is solvable because both its normal subgroup $H = \text{Gal}(E/F)$ and the quotient $G/H = \text{Gal}(F/\mathbb{Q})$ are abelian.
5. Let $S$ denote the set of primes less than 20, let

$$f(x) = \prod_{p \in S} (x^2 - p)$$

and let $E$ be the splitting field of $f(x)$ over $\mathbb{Q}$.

(a) (10 points) What is $G = \text{Gal}(E/\mathbb{Q})$?

**Solution:** The zeros of $f(x)$ are the positive and negative square roots of the primes in $S$. For each such prime $p$ there is an automorphism $\phi_p$ sending $\sqrt{p}$ to $-\sqrt{p}$ and fixing the other zeros. Since there are 8 primes in $S$, $G = C_2^8$.

(b) (10 points) How many subgroups of index 2 does $G$ have?

**Solution:** Each such subgroup is the kernel of a nontrivial homomorphism $\chi : G \to C_2$. Each such homomorphism is determined by its behavior on the eight $\phi_p$s, and $\chi(\phi_p)$ has two possible values for each prime $p$. Hence there are $2^8$ such homomorphisms including the trivial one, so there are 255 subgroups of index 2.

(c) (10 points) Identify the subfields of $E$ fixed by these subgroups.

**Solution:** Let $P = \prod_{p \in S} p$, the product of all the primes under 20, also known as 9,699,690. It has 255 divisors other than 1, one for each nonempty subset of $S$, the divisor being the product of the primes in the subset. Call this set of divisors $D$. Then our collection of subfields is

$$\left\{ \mathbb{Q}(\sqrt{d}) : d \in D \right\}.$$

You may think of another description.