77. Construct a field of (a) 8; (b) 25; (c) 32 elements.

78. Let F be a finite field. Prove the following statements:
(a) There exists a unique prime number p such that any $c \in F$ added p times gives 0.
(b) F contains a subfield isomorphic to $\mathbf{Z}_p$.
(c) F is a vector space over this subfield under the natural operations.
(d) The number of elements in F is a prime power.

79. Let F be a finite field of n elements. Prove:
(a) $c^{n-1} = 1$ for every non-zero $c \in F$.
*(b) There exists a non-zero $\alpha \in F$ such that $\alpha^k \neq 1$ for every $0 < k < n-1$.
(c) $F = \{0, \alpha, \alpha^2, \ldots, \alpha^{n-2}, \alpha^{n-1} = 1\}$ for some $\alpha \in F$, i.e. all non-zero elements are powers of a suitable element α.
(d) $\alpha^r = \alpha^t \iff r \equiv t \pmod{n-1}$.

80. Determine the sum and product of the non-zero elements of a finite field.

81. In which finite fields is every element a square?

82. Find all finite fields where we can take the square of a sum by terms, i.e. $(a+b)^2 = a^2 + b^2$ holds for every a, b? Solve the similar problem when squares are replaced by cubes. (*) Generalize for pth powers where p is a prime (try first, say, $p = 7$).

83. A set of integers $1 \leq a_1 < a_2 < \ldots < a_k \leq n$ is called a *Sidon set* if the sums $a_i + a_j$ $(i \leq j)$ are pairwise distinct. Our aim is to give upper and lower bounds for the maximal size $k = s(n)$.
(a) Show that the condition is equivalent to the differences $a_i - a_j$ $(i \neq j)$ being pairwise distinct.
(b) Upper bounds: (b1) $k \leq 2\sqrt{n}$; moreover (b2) $k \leq \sqrt{2n} + 1$.
(c) Lower bounds: (c1) $k \geq \log_2 n$; moreover (c2) $k \geq \sqrt[3]{n}$.
(d) Improved lower bound for $n = p^2 - 1$ where p is a prime: $k \geq p = \lceil \sqrt{n} \rceil$.
(d1) At most how many numbers can be selected satisfying the stronger requirement that the differences $a_i - a_j$ $(i \neq j)$ are (not just pairwise distinct but are even) pairwise incongruent mod n?
*(d2) Prove that there exist p elements satisfying this stronger requirement.