(i) The number of elements in a finite field F is a prime power p^k $(k \geq 1)$, and to every p^k there exists (up to isomorphism) exactly one finite field of that size.
(ii) Additive structure: There is a unique prime p such that adding any element p times gives 0.
(iii) Multiplicative structure: There exists a so-called *"primitive" element* α such that every non-zero element is a power of α: $F = \{0, \alpha, \alpha^2, \ldots, \alpha^{n-2}, \alpha^{n-1} = 1\}$ where $|F| = n$. Hence $\alpha^r = \alpha^t \iff r \equiv t \pmod{n-1}$. There are $\varphi(n-1)$ such primitive elements where $\varphi(s)$ is Euler's function counting the coprime elements to s among the numbers $1, 2, \ldots, s$. The primitive elements in $\mathbf{Z}_p$ are called *primitive roots*.
(iv) Subfield: F contains a subfield isomorphic to $\mathbf{Z}_p$, hence F is a vector space over this subfield.
(v) Construction of a field F of size p^k: $\mathbf{Z}_p[x]/(f)$ where f is an irreducible polynomial over $\mathbf{Z}_p$ of degree k.

Sidon sets

A (finite or infinite) sequence of positive integers $a_1 < a_2 < \ldots$ 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 $k = s(n)$ of a Sidon set contained in the interval $[1, n]$. The best results show that $\lim_{n\to\infty} s(n)/\sqrt{n} = 1$. Erdős offers \$1000 for determining whether $|s(n) - \sqrt{n}|$ is bounded, or not.

Upper bounds:

(U1) There are $\binom{k}{2} + k = k(k+1)/2$ sums $a_i + a_j$, all contained in the interval $[2, 2n]$. Since each sum is a different integer, therefore $k(k+1)/2 \leq 2n - 1$, which implies $k^2 < 4n$, i.e. $s(n) < 2\sqrt{n}$.

(U2) Since $a_i + a_j = a_r + a_s \iff a_i - a_r = a_s - a_j$, also the differences $a_i - a_j$ $(i > j)$ are pairwise distinct, and each difference is in the interval $[1, n-1]$. Thus $\binom{k}{2} \leq n - 1$, hence $(k - 1/2)^2 \leq 2n - 7/4$, i.e. $s(n) < \sqrt{2n} + 1/2$.

(U3) Erdős and Turán proved by elementary methods, using the Cauchy-inequality, that $s(n) \leq \sqrt{n} + \sqrt[4]{n} + 1$.

Lower bounds:

(L1) The powers of 2 clearly form a Sidon set, hence $s(n) \geq 1 + \lfloor \log_2 n \rfloor$.

(L2) We construct a Sidon set using the greedy algorithm: we pick always the first number available $(1, 2, 4, 8, 13, \ldots$; we cannot take 3, because $3 + 1 = 2 + 2$, we cannot take 5, because $5 + 1 = 4 + 2$, etc.). If we have already selected $a_1, \ldots, a_{k-1}$, then the solutions x of $x + a_s = a_r + a_t$, i.e. $x = a_r + a_t - a_s$ (*) $(r, s, t \leq k-1)$ are the forbidden values for a_k (these include also the numbers $x = a_r = a_r + a_s - a_s$). In (*) there are at most $\binom{k-1}{2} + (k-1)$ choices for a_r and a_t, and at most $k-1$ choices for

a_s. Hence at most $k^3/2$ values are forbidden, which means that we certainly have a suitable a_k, as long as $k^3/2 < n$, i.e. $k < \sqrt[3]{2n}$. Therefore $\max k = s(n) \geq \sqrt[3]{2n}$.

(L3) If p is an odd prime, then for $n = 2p^2$ we construct a Sidon set of size $p = \sqrt{n/2}$. For general n we can use the largest $2p^2 \leq n$, hence we obtain asymptotically $\sqrt{n/2}$ as a lower bound for $s(n)$.

The construction: $a_i = 1 + 2pi + [i^2]$ $(i = 0, 1, \ldots, p-1)$, where $[i^2]$ means the (least non-negative) residue of i^2 mod p: $a_0 = 1$, $a_1 = 2p + 2$, etc.

To prove the Sidon property, assume $a_i + a_j = a_r + a_s$. We have to show that either $i = r, j = s$, or $i = s, j = r$. By the definition of the a-s, $0 = 2p(i + j - r - s) + ([i^2] + [j^2] - [r^2] - [s^2]) = 2pA + B$. Here $2p \mid B$, but $|B| < 2p$, hence $B = 0$, and also $A = 0$. Rearranging these equalities, we obtain $i - r = s - j$ and $i^2 - r^2 \equiv s^2 - j^2 \pmod{p}$. We are done, if $i - r = s - j = 0$. Otherwise we can divide the congruence by the common value $i - r = s - j$ (*), and obtain $i + r \equiv s + j \pmod{p}$ (**). Adding and subtracting (*) and (**), and dividing by 2, we arrive at $i = s, r = j$.

(L4) If p is an odd prime, then for $n = p^2 - 1$ we construct a Sidon set of size $p = \lceil \sqrt{n}\, \rceil$. For general n we use the largest $p^2 - 1 \leq n$, hence we obtain asymptotically $\sqrt{n}$ as a lower bound for $s(n)$. Moreover, using deep number theoretical results about the difference of the consecutive primes, we have $s(n) \geq \sqrt{n} - n^{0.27}$.

In fact, we shall prove more for $n = p^2 - 1$: we construct elements $a_1, \ldots, a_p$, such that the differences $a_i - a_j$ $(i \neq j)$ are pairwise incongruent mod n. (We cannot have more numbers with this property, since $(p+1)p > p^2 - 2$.)

For the construction, we use the field $F = F_{p^2}$ of p^2 elements. Let α be a primitive element in F, i.e. each non-zero element of F is of the form α^j, where j is uniquely determined mod $p^2 - 1$. Let c_i be the elements of $\mathbf{Z}_p \subset F$, and define a_i as the exponent of α representing the element $\alpha + c_i$, i.e. $\alpha^{a_i} = \alpha + c_i$, $i = 1, 2, \ldots, p$.

Now, if $a_i + a_j \equiv a_r + a_s \pmod{p^2 - 1}$, then

$$(\alpha + c_i)(\alpha + c_j) = \alpha^{a_i + a_j} = \alpha^{a_r + a_s} = (\alpha + c_r)(\alpha + c_s),$$

i.e. $(c_i + c_j - c_r - c_s)\alpha + (c_i c_j - c_r c_s) = 0$. Since $\alpha \notin \mathbf{Z}_p$, this implies $c_i + c_j - c_r - c_s = c_i c_j - c_r c_s = 0$, and hence the (unordered) pairs $\{i, j\}$ and $\{r, s\}$ are the same.

We note the following variants: (A) For $n = p^2 + p + 1$ we can construct elements $a_1, \ldots a_{p+1}$, such that the differences $a_i - a_j$ $(i \neq j)$ are pairwise incongruent mod n (hence each non-zero residue has a unique representation as $a_i - a_j$). We use the fact, that two non-zero elements, α^i and α^j, are linearly dependent in F_{p^3} iff $i \equiv j \pmod{p^2 + p + 1}$.

(B) For $n = p^2 - p$ we can construct elements $a_1, \ldots, a_{p-1}$, such that the differences $a_i - a_j$ $(i \neq j)$ are pairwise incongruent mod n. Here we use a primitive root g mod p, and a_i is the solution of the system of congruences $x \equiv i \pmod{p-1}$, $x \equiv g^i \pmod{p}$, $i = 1, 2, \ldots, p-1$.

freud@caesar.elte.hu freud.web.elte.hu/bsm/index.html