Factoring method chronology

1967: hard 27-digit factorizations are intractible

1975: first asymptotically subexponential method, CFRAC

1977: RSA appears in Scientific American, 129-digit
challenge to break RSA129

1981-1983: Quadratic Sieve at Sandia Nat'l Labs (Cray 1)

69-digit composite factored; last of Mersenne's list
Time Magazine, 1983.

1988-1991: MPQS, ppmpqs at Digital Research (Lenstra-Mannasse)

hard 100-digit number factored; first distributed
internet computation (E-mail factorization). Workstations.

1991: special 512-bit factorization, $2^{(2^9)} + 1 = 2^{512} + 1$,
start of number field sieve (NFS)

addendum: Algebraic primes. (i) among complex numbers $a + bi, i = \sqrt{-1}$ with a, b integers, the **Gaussian integers,** the rational prime 5 factors as $5 = (2 + i)(2 - i)$, where $\pi_5 = 2 + i$ is an algebraic prime — it's only divisors are $\pm 1, \pm i, \pm \pi_5$, and $\pm i\pi_5$.

(ii) For $\alpha = \sqrt[5]{2}$, the integers are $n_0 + n_1\alpha + \cdots + n_4\alpha^4$, with n_i integers, and the prime 2 factors $\alpha \cdot \alpha^4$, as used with the special NFS.

(iii) For general numbers, like RSA-512, we use α a root of a 5th degree polynomial with 16- to 20-digit coef., and again integers $n_0 + n_1\alpha + \cdots + n_4\alpha^4$.