61) Factorize 12968419 with the quadratic sieve, using the factor base 3, 5, 7, 19, 29 and a sieving interval of length 2 \cdot 80.

62*) Show that if \( n \) is odd, composite and not a prime power, then at least half of the pairs \( x, y \) with \( 0 \leq x, y < n \) and \( x^2 \equiv y^2 \pmod{n} \) have \( 1 < \gcd(x - y, n) < n \).

63) Suppose that \( n \) is a number that has a prime factor \( p \), such that \( p - 1 \) is a product of small primes.
   a) Let \( k = 2^{e_2}3^{e_3} \cdots p_k^{e_k} \) a product of powers of the first \( k \) primes (for example let \( k \) be the LCM of the first \( m \) numbers). Show that if \( p - 1 | k \) then \( \gcd(a^k - 1, n) \geq p > 1 \) for any \( a \) coprime to \( n \).
   b) Use this approach to factor 387598193 into prime numbers, using a base \( a = 2 \) and \( k = \text{lcm}(2,3,\ldots,8) \). (This method is also due to Pollard and is called the \( p - 1 \)-method. A generalization is the Elliptic Curve Factorization Algorithm by H. Lenstra, which is the best known “all-purpose” method, if the number has smaller prime factors.)

64) Use the principle of inclusion/exclusion to give a formula for the number of squarefree integers less than or equal to \( n \).

65) Calculate \( \pi(150) \) using Legendre’s formula.

Problems marked with a * are bonus problems for extra credit.

The quadratic sieve in GAP

The \texttt{factint} share package for GAP implements (among other) the quadratic sieve factoring algorithm and provides a better general method for \texttt{Factors}. This package should load automatically (it is installed on the PCs in the lab and should also be available if you installed GAP from a CD you got from me). (Note: Since \texttt{factint} installs a better method for \texttt{Factors}, you cannot compare the performance of \texttt{Factors} with and without this package loaded.) You can get information about the factorization process by setting

\[
gap> \text{SetInfoLevel(IntegerFactorizationInfo,2);}
\]

The function \texttt{FactorsMPQS} implements the multipolynomial quadratic sieve (it uses initially Pollard’s \( \rho \)-method to get smaller factors). For example:

\[
\text{gap> FactorsMPQS(1044396320275711827781205923);}
\]
\[
[ 48742642651, 21426747986432473 ]
\]

An old final

1) Find by hand all solutions to the following congruences:
   a) \( 4x + 7 \equiv 5 \pmod{19} \)  \quad b) \( 12x \equiv 18 \pmod{30} \)
2) Show that for every even \( n \geq 6 \) there exist primes \( p \) and \( q \) such that \((n - p, n - q) = 1\).

3) Determine all nonprime integers \( n \), such that \( \phi(n) = pq \) is the product of two primes.

4) Determine (without using a ChineseRem function) a solution to the following set of congruences: \( x \equiv 3 \pmod{5} \), \( x \equiv 2 \pmod{11} \), \( x \equiv 1 \pmod{23} \).

5) a) Determine (without using an OrderMod function) the orders of 2 and 11 modulo 257. b) Let \( n = 110881 \) (which is prime). You are given the information that \( \text{ord}_n(15) = 990 \) and \( \text{ord}_n(17) = 7392 \). Determine (without using a PrimitiveRoot function) a primitive root modulo \( n \).

6) Show (without explicitly testing all bases) that \( 6601 = 7 \cdot 23 \cdot 41 \) is a Carmichael number.

7) Let \( n = 1019 \) (which is prime). a) Show that 2 is a primitive root modulo \( n \). b) Using Shanks's algorithm, determine the index \( \text{ind}_2(470) \). c) Determine all solutions of the equation \( x^6 \equiv 470 \pmod{1019} \).

8) a) Show that 1729 is a pseudoprime for base 2 but not a strong pseudoprime for base 2. b) Show that \( p = 123456791 \) is probably prime, by showing that is is a strong pseudoprime for (at least) 5 bases. Can you deduce that it is prime? c) Prove that 1237 is prime, using the Lucas-Lehmer test (you may assume knowledge of all primes < 100).

9) Using the Quadratic Reciprocity Law, determine whether the following equations have a solution (You may assume that all moduli are prime). you do not need to give the solutions:
   a) \( x^2 \equiv -1 \pmod{1237} \)
   b) \( x^2 \equiv 44100 \pmod{1234577} \)
   c) \( x^2 \equiv 93732 \pmod{1234577} \)

10) We want to factorize \( 42448001 \) with the quadratic sieve.
    a) Determine all primes smaller than 18 which can be factors of \( x^2 - n \).
    b) Write down a sieving table for a factor base given by the primes in a), and a sieving interval of length \( 2 \cdot 10 \).
    c) Factorize \( 42448001 \) with the quadratic sieve. (You do not need to prove that the factors are prime.)

11) Show that for any integer \( n > 1 \) the decomposition of \( n! \) into prime factors contains at least one prime with exponent 1.

12) State (assuming only the knowledge of a student at the start of M400):
    a) The Riemann Hypothesis.
    b) The definition of a nonsingular elliptic curve.