Exercise 1.7
... compute the following quotients and remainders.
(a) 34787 divided by 353.
(b) 238792 divided by 7843.
(c) 9829387493 divided by 873485.
(d) 1498387487 divided by 76348.

Exercise 1.8
... compute the following remainders, without bothering to compute the associated quotients.
(a) The remainder of 78745 divided by 127.
(b) The remainder of 2837647 divided by 4387.
(c) The remainder of 8739287463 divided by 18754.
(d) The remainder of 4536782793 divided by 9784537.

Exercise 1.9
Use the Euclidean algorithm to compute the following greatest common divisors.
(a) gcd(291,252).
(b) gcd(16261,85652).
(c) gcd(139024789,93278890).
(d) gcd(16534528044,8332745927).

Exercise 1.12(c)
Use your program to compute g=gcd(a,b) and integer solutions to the equation au+bv=g for the following pairs (a,b).
(i) (527,1258)
(ii) (228,1056)
(iii) (163961,167181)
(iv) (3892394,239847)

Exercise 1.28
Compute the following ord_p values. (qui ord_p(x) = ordine di x in Z_p)
(a) Compute ord_2(2816).
(b) Compute ord_7(2222574487).
(c) Compute ord_p(46375) for each of p=3, 5, 7, and 11.

Exercise 2.28
Use the Baby-Step-Giant-Step algorithm (or the Pohlig–Hellman Algorithm) to solve the discrete logarithm problem...

(a) p = 433, g = 7, a = 166.
(b) p = 746497, g = 10, a = 243278.
(c) p = 41022299, g = 2, a = 39183497. (Hint: p=2*295+1.)
(d) p = 1291799, g = 17, a = 192988. (Hint: p–1 has a factor of 709.)

Exercises 3.5(b)
Solve the following congruences. ...
(i) x577 ≡ 60 (mod 1463).
(ii) x959 ≡ 1583 (mod 1625).
(iii) x133957 ≡ 224689 (mod 2134440).

Exercises 3.8
For each of the given values of N=pq and (p-1)(q-1), use the method described in Remark 3.10 to determine p and q.(a) N = pq = 352717 and (p – 1)(q – 1) = 351520.
(b) N = pq = 77083921 and (p – 1)(q – 1) = 77066212.
(c) N = pq = 109404161 and (p – 1)(q – 1) = 109380612.
(d) N = pq = 172205490419 and (p – 1)(q – 1) = 172204660344.

Exercises 3.9
A decryption exponent for an RSA public key (N,e) is an integer d with the property that...
(b) Let N = 38749709. Eve's magic box tells her that the encryption exponent e = 10988423 has decryption exponent d = 16784693 and that the encryption exponent e = 25910155 has decryption exponent d = 11514115. Use this information to factor N.
(c) Let N = 225022969. Eve's magic box tells her the following three encryption/decryption pairs for N: (70583995,4911157), (173111957,7346999), (180311381,29597249). Use this information to factor N.
(d) Let N = 1291233941. Eve's magic box tells her the following three encryption/decryption pairs for N: (1103927639,76923209), (1022313977,106791263), (387632407,7764043). Use this information to factor N.

Exercises 3.12
Alice decides to use RSA with the public key N = 1889570071. In order to guard against transmission errors, Alice has Bob encrypt his message twice, once using the encryption exponent e1 = 1021763679 and once
using the encryption exponent e2 = 519424709. Eve intercepts the two encrypted messages c1=1244183534 and c2=732959706. Assuming that Eve also knows N and the two encryption exponents e1 and e2, ... help Eve recover Bob's plaintext without finding a factorization of N.

Exercises 3.14
Use the Miller–Rabin test on each of the following numbers. ...
(a) n = 1105.
(b) n = 294409.
(c) n = 294439.
(d) n = 118901509.
(e) n = 118901521.
(f) n = 118901527.
(g) n = 118915387.

Exercises 3.21
Use Pollard's p–1 method to factor each of the following numbers.
(a) 1739 (b) 220459 (c) 48356747

Exercises 3.27(c)
The following is a list of 20 randomly chosen numbers between 1 and 1000, sorted from smallest to largest. Which of these numbers are 10-power-smooth? Which of them are 10-smooth?
{84, 141, 171, 208, 224, 318, 325, 366, 378, 390, 420, 440, 504, 530, 707, 726, 758, 765, 792, 817}

Exercises 5.18
Use the Elliptic Curve Factorization Algorithm to factor each of the numbers N using the given

elliptic curve E and point P.

(a)N=589, E:Y^2 =X^3 +4X+9, P=(2,5).
(b)N=26167, E:Y^2 =X^3 +4X+128, P=(2,12).
(c)N=1386493, E:Y^2 =X^3 +3X–3, P=(1,1).
(d)N=28102844557, E:Y^2 =X^3 +18X–453, P=(7,4).