GEORGIA TECH MATH, PHYSICS & COMPUTING

MATH 4803BDU,BDG, CS4803F, PHYS4803A

QUANTUM INFORMATION & QUANTUM COMPUTING

Problems Set 4

Due March 20th, 2003

Arithmetic and prime number decomposition :

$\mathbb{N} = \{0, 1, 2, 3, \cdots, \}$ denotes the set of *natural* (or *positive* or *non negative*) integers. $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$ denotes the set of all integers endowed with its canonical structure of *ring* (addition and multiplication). If $a, b \in \mathbb{Z}$, then a *divides* b (and this is denoted by $a|b$) whenever there is an integer d such that $b = ad$. a is called a *factor* or a *divisor* of b. Clearly, 1 is always a factor of any integer and any integer always divides itself. An integer $p > 1$ is a *prime number* if it has no divisors other than 1 and itself. Example of prime numbers are $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \cdots\}$. It is known that there is an infinite number of prime numbers. Moreover the prime number theorem asserts that there are $O(x/\ln x)$ prime numbers between 2 and x. The *fundamental theorem of arithmetic* (see question (1d) below) asserts that each positive integer can be decomposed in a unique way into product of powers of prime numbers. One difficult question is whether it is possible to find a fast algorithm that produces this decomposition for a given integer n. Only very recently did three Indian computer scientists find an algorithm solving this problem in a polynomial time in n. The purpose of this problem is to give a quantum algorithm solving this problem in a time $O(L^3) = O((\ln n)^3)$ if L is the minimum number of binary digits needed to write n.

1. (a) Show that if d divides both a and b, then it divides $ax + by$ for any $x, y \in \mathbb{Z}$.
   (b) Show that if $a, b \in \mathbb{N}$, then $a|b \Rightarrow a \leq b$.
   (c) Show that the relation $a|b$ is an *order relation* on $\mathbb{N}$.
   (*Namely (i)* $a|a$, *(ii)* $a|b$ *and* $b|a \Rightarrow a = b$ *; (iii)* $a|b$ *and* $b|c \Rightarrow a|c$.)
   (d) Prove the *fundamental theorem of arithmetic* : any integer $n > 1$ can be decomposed in a unique way into a product of powers of prime numbers, namely
   $$n = \prod_{p \in \mathcal{P}} p^{\alpha_p} = p_1^{\alpha_{p_1}} \cdots p_m^{\alpha_{p_m}} ,$$
   where $\underline{\alpha}(n) = (\alpha_p)_{p \in \mathcal{P}}$ is a family of natural integers, a finite number of which only being non zero.
   (e) If $a \in \mathbb{N}$, characterize all its divisors in term of its prime decomposition.
2. Let x be an integer. For any integer $n > 1$ show that there is a unique integer $k \geq 0$ such that $kn \leq x < (k+1)n$. k is called the *division of x by n*. The difference $x - kn = r$ is called the *rest*. Show that the decomposition $x = kn + r$ with $0 \leq r \leq n - 1$ is unique.
3. Two integers $x, y \in \mathbb{Z}$ are *equal modulo n* (notation $x = y \pmod{n}$) whenever $x - y$ is an integer multiple of n.

(a) Show that the relation $x = y \pmod{n}$ is an equivalence relation between integers.

(b) Show that $x = r \pmod{n}$ if r is the rest of the division of x by n.

(c) Show that each equivalence class contains one element $\{0, 1, \cdots, n-1\}$ and only one. The set of such equivalence classes is denoted by $\mathbb{Z}_n$. How many elements does $\mathbb{Z}_n$ contain ?

(d) Show that the equivalence classes of $x+y$ and of xy depends only upon the equivalence classes of x and of y. Hence addition and multiplication modulo n is well defined.

(e) Show that, endowed with addition and multiplication modulo n, $\mathbb{Z}_n$ is a *ring*. What is the element of $\{0, 1, \cdots, n-1\}$ representing -1 ?

(f) Given the multiplication table of $\mathbb{Z}_{21}$.

(g) Give the list of invertible elements of $\mathbb{Z}_{21}$? Give the solutions of $x^2 = 1 \pmod{21}$ other than ± 1.

4. Given a and b two natural integers, then $\gcd(a, b)$ denotes their *greatest common divisor.*

   (a) If $a = \prod_p p^{\alpha_p}$ and $b = \prod_p p^{\beta_p}$ are the prime decompositions of a and b, give the prime decomposition of $\gcd(a, b)$.

   (b) Show that $\gcd(a, b)$ is the smallest positive integer s that can be written as $s = ax+by$ for $x, y \in \mathbb{Z}$. In particular a and b are co- prime if and only if there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$ (*Bezout's theorem*).
   (*Hint : show first that* $\gcd(a, b)$ *is a divisor of* s*. Then show, by contradiction, that* s *is a common divisor of* a *and* b*.*)

   (c) Show that if c divides both a and b, then it divides $\gcd(a, b)$.

5. Two integers a, b are *co-prime* whenever $\gcd(a, b) = 1$.

   (a) Prove that x is invertible $\pmod{n}$ if and only if x and n are co-prime.

   (b) Prove that, if a is invertible $\bmod n$, its inverse is unique in $\mathbb{Z}_n$.

   (c) If p if prime, prove that all non zero elements of $\mathbb{Z}_p$ are invertible. In particular $\mathbb{Z}_p$ is a *field* denoted by $\mathbb{F}_p$.

   (d) Show that, if $n \in \mathbb{N}$ is greater than 1, $(n + 1)$ is always invertible $\bmod(n^2)$ and give its inverse.

6. The *Euclid algorithm* is a way to compute the $\gcd(a, b)$ for $a, b \in \mathbb{N}$. It is enough to assume that $a > b$.

   (a) Prove that if r denotes the rest of the division of a by b, $\gcd(a, b) = \gcd(b, r)$.
   (*Hint : use the result of question (4c).*)

   (b) Show that replacing a by b and b by r, and iterating this procedure, then one gets a *finite sequence* $r_1 = r > r_2 > \cdots > r_m$ such that $\gcd(a, b) = \gcd(r_i, r_{i+1}) = r_m$.

   (c) Compute $\gcd(2002, 1946)$.

   (d) Show that $r_{i+2} \le r_i/2$. (*Hint : consider the two cases* $r_{i+1} \le r_1/2$ *and* $r_{i+1} > r_1/2$.)

   (e) Show then that if a requires L binary digits to be written, then the Euclid algorithm can be achieved in $m = O(L)$ steps. If one assumes that each step (divide-and-rest operations) requires $O(L^2)$ elementary computer operations, then what is its cost in computer time ?

(f) How can one use the Euclid algorithm to find efficiently two integers x, y such that $\gcd(a, b) = ax + by$? What is the cost of this problem?

(g) Show that the Euclid algorithm can also been used to compute efficiently the inverse of $a \pmod{n}$, whenever a and n are co-prime.

7. *The Chinese remainder theorem* : let $m_1, \cdots, m_k$ be pairwise co-prime positive integers. Let $a_1, \cdots, a_k$ be integers.

   (a) Prove that there is $x \in \mathbb{Z}$ such that x is a solution of

   $$x = a_1 \pmod{m_1}\,, \quad \cdots \quad , x = a_k \pmod{m_k}\,.$$

   (b) Show that two such solutions are equal $\bmod (m_1 \cdots m_k)$.

8. The *Euler φ-function* gives, for $n \in \mathbb{N}$, the number $\varphi(n)$ of positive integers co-prime to n.

   (a) Show that $\varphi(n) < n$.

   (b) If p is prime, what is $\varphi(p)$?

   (c) If $\alpha \in \mathbb{N}$ and $p \in \mathcal{P}$, compute $\varphi(p^\alpha)$.

   (d) If $a, b \in \mathbb{N}$ are co-prime, show that $\varphi(ab) = \varphi(a)\varphi(b)$.
   (*Hint : use the Chinese remainder theorem.*)

   (e) Prove that

   $$n = \sum_{d; d|n} \varphi(d)\,.$$

   (*Hint : prove it for powers of prime numbers, then use the factorization property*)

9. Let n be a positive integer and let $1 < x < n - 1$ be a solution of $x^2 = 1 \pmod{n}$.

   (a) Then show that $x \neq \pm 1 \pmod{n}$.

   (b) Show that at least one of $\gcd(x - 1, n)$ and $\gcd(x + 1, n)$ is a non trivial factor of n.

   (c) If n can be expressed with L binary digits, show that computing $\gcd(x \pm 1, n)$ can be performed in $O(L^3)$ operations.

10. Let $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ be a factorized integer. Let $x \in \{2, \cdots, n - 2\}$ be chosen at random (namely with uniform probability) among the integers co-prime to n. Then let r be the order of x, namely r is the smallest non zero integer such that $x^r = 1 \pmod{n}$.

    (a) What is the number of such x's? What is the probability of choosing x then?

    (b) Prove that the probability that $x^{r/2} \neq -1 \pmod{n}$ is larger than or equal to $1 - 1/2^m$.

11. Give now an algorithm, using the quantum *order finding* method to find one non trivial factor of n with no more than $O(L^3)$ operations if L is the number of binary digits needed to express n.

Georgia Tech

Math, Physics & Computing
Math 4803BDU,BDG, CS4803F, Phys4803A

Quantum Information & Quantum Computing

Correction, Problems Set

Arithmetic and prime number decomposition :

In this problem $\mathbb{N}_*$ denotes the set of non zero positive integers.

1. (a) If d divides both a and b there are integers a', b' such that $a = da'$ and $b = db'$. Thus $ax + by = d(a'x + b'y)$ for any pair $x, y \in \mathbb{Z}$. Since $a'x + b'y$ is an integer, it follows that d divides $ax + by$.

   (b) If $a, b \in \mathbb{N}_*$ are positive integers such that $a|b$ then, there is $d \in \mathbb{Z}$ such that $b = ad$ Thus d must be positive as well. Since $b \neq 0$ then $d \geq 1$ so that $a \leq ad = b$.

   (c) All integers will be assumed in $\mathbb{N}_*$. It is clear that $a|a$ since $a = a \cdot 1$ and $1 \in \mathbb{N}_*$. Moreover if $a|b$ and $b|a$ then there are $d, d' \in \mathbb{N}_*$ such that $b = ad$ and $a = bd'$. It follows that $a = add'$ so that $dd' = 1$ which happens only if $d = d' = 1$. Hence $a = b$.

   (d) If n is prime, then there is nothing to be proved. If n is not prime, then let m_1 be a non trivial divisor of n, that is $1 < m_1 < n$, so that $n = m_1 n_1$ for some $n_1 \in \mathbb{N}_*$, $n_1 > 1$. By recursion, it is possible to get a decreasing sequence $m_1 > m_2 > \cdots > m_k > 1$ such that $m_{i+1}|m_i$ and therefore $n = m_k n_k$ for some $n_k \in \mathbb{N}_*$. This sequence must terminate, so that m_k has no other divisor than 1 and itself, namely m_k is prime. Therefore $1 < n_k < n$. Replacing now n by n_k leads to a decomposition of n into a product of prime numbers. If p is such prime, p appears in general several times. Let $\alpha_p \in \mathbb{N}$ be this occurence number. Then p^{α_p} is a divisor of n. Therefore setting $\alpha_p = 0$ if p never occur in this decomposition, n can be written as

   $$n = \prod_{p \in \mathcal{P}} p^{\alpha_p} .$$

   Let now $n = \prod_{p \in \mathcal{P}} p^{\beta_p}$ be another such decomposition. Then if $p \in \mathcal{P}$ occurs with $\alpha_p > 0$, then n/p^{α_p} is an integer, so that $\beta_p \geq \alpha_p$. By the same argument, exchanging the roles of the two decompositions, $\alpha_p \geq \beta_p$ also, so that $\alpha_p = \beta_p$. This proves the uniqueness.

   (e) It follows from the previous argument that if m divides n, its prime number decomposition $m = \prod_{p \in \mathcal{P}} p^{\beta_p}$ must satisfy $\beta_p \leq \alpha_p$ for all prime p. Conversely, if $0 \leq \beta_p \leq \alpha_p$ for all prime p, then m divides n.

2. Given $n > 1$ and $x \in \mathbb{Z}$, there is a largest $k \in \mathbb{Z}$ such that $kn \leq x$. Then, by the very definition of the maximum, $(k+1)n > x$. It follows that $x = kn + r$ where $r = x - kn$ so that $0 \leq r < n$. This prove the existence. If $x = kn + r = k'n + r'$ with $0 \leq r, r' < n$, then let choose them so that $r \leq r'$. It follows that $r' - r = (k - k')n$ and that $0 \leq r' - r \leq r' < n$. Thus the only possibility is $k = k'$ so that $r = r'$. This prove uniqueness.
3. (a) Clearly $x = x\,(\mathrm{mod}\,n)$ since $x - x = 0 = 0 \cdot n$. Moreover if $x = y\,(\mathrm{mod}\,n)$ then $x - y = kn$ for some $k \in \mathbb{Z}$, so that $y - z = -kn$ showing that $y = x\,(\mathrm{mod}\,n)$. Hence the relation is symmetric. If now $x = y\,(\mathrm{mod}\,n)$ and $y = z\,(\mathrm{mod}\,n)$, then there are $k, l \in \mathbb{Z}$ such that $x - y = kn$, $y - z = ln$. Hence $x - z = (k+l)n$ so that $x = z\,(\bmod\ n)$. Therefore the relation is also transitive, namely it is an equivalence relation.

   (b) If $x = kn + r$ is the result of the euclidean division of x by n, then $x - r = k \cdot n$ namely $x = r\,(\mathrm{mod}\,n)$.

   (c) The previous question shows that any $x \in \mathbb{Z}$ is equivalent $(\bmod\ n)$ to its rest, namely to an element of the finite set $\{0, 1, \cdots, n-1\}$. On the other hands if both r and r' belong to this set, either $r \leq r'$ so that $0 \leq r' - r \leq n - 1$, or $r' \leq r$ so that $0 \leq r - r' \leq n - 1$. In both cases, $r = r'\,(\mathrm{mod}\,n)$ implies $r = r'$. Therefore x is equivalent to one and only one element of this set. This shows that the set $\mathbb{Z}_n$ of equivalent classes $(\bmod\ n)$ is bijectively represented by $\{0, 1, \cdots, n-1\}$, in particular $\mathbb{Z}_n$ contains exactly n elements.

   (d) If $x, y \in \mathbb{Z}$, with $x = kn + r$ and $y = ln + s$ where $0 \leq r, s \leq n - 1$, then $x + y = (k+l)n + r + s$ so that $x + y = r + s\,(\mathrm{mod}\,n)$. Thus the equivalence class $[x + y]$ of $x + y$ depends only upon the equivalence class of the sum $r + s$ of the rests namely of the equivalence classes $[x]$ of x and $[y]$ of y. Note that either $r + s < n$ and $r + s$ is the representative of $x + y$, or $n \leq r + s \leq 2n - 2$ and then $0 \leq r + s - n \leq n - 1$ is the representative of $x + y$[1].

   (e) The previous question shows that there is a well defined addition $([x], [y]) \in \mathbb{Z}_n \times \mathbb{Z}_n \mapsto [x] + [y] := [x + y] \in \mathbb{Z}_n$ where $[x + y]$ is represented by $r + q - \epsilon_{r,s}n$ (for $\epsilon_{r,s} \in \{0, 1\}$) if r and s are the rests of the euclidean division of x and y by n respectively. This is an abelian group law, because

      i. it is associative : $([x] + [y]) + [z] = [x + y] + [z] = [(x + y) + z] = [x + (y + z)] = [x] + [y + z] = [x] + ([y] + [z])$[2], where the associativity of the addition in $\mathbb{Z}$ has been used ;

      ii. the equivalent class of 0, represented by 0 in $\{0, 1, \cdots, n-1\}$ is the neutral element since $[x] + [0] = [x + 0] = [x]$;

      iii. every element has an opposite, $[-x] = -[x]$ since $[x] + [-x] = [x - x] = [0] = 0$; in particular $-[1] = [n - 1]$ so that $n - 1$ is the representative of $-[1]$ in $\{0, 1, \cdots, n-1\}$;

      iv. it is abelian since $[x] + [y] = [x + y] = [y + x] = [y] + [x]$, using the commutativity of the sum in $\mathbb{Z}$;

[1]The addition in base n is using an algorithm based on this remark

[2]this is equivalent to say that $([x]+[y])+[z]$ is represented by $r+s-\epsilon_{r,s}n+t-\epsilon_{r+s-\epsilon_{r,s},t}n = r+s+t\,(\bmod\ n)$, if t is the rest of the euclidean division of z by n, whereas $[x]+([y]+[z])$ is represented by $r+s+t-\epsilon_{s,t}n-\epsilon_{r,s+t-\epsilon_{s,t}} = r + s + t\,(\mathrm{mod}\,n)$. Thus $([x] + [y]) + [z] = [x] + ([y] + [z])$

In very much the same way, there is a multiplication defined by $([x],[y]) \in \mathbb{Z}_n \times \mathbb{Z}_n \mapsto [x]\cdot[y] := [xy] \in \mathbb{Z}_n$. For indeed, $xy = (kn+r)(ln+s) = (kln+ks+rl)n + sr = rs \,(\mathrm{mod}\, n)$, so that the equivalence class of xy depends only upon the rests r, s of their euclidean division by n, namely upon their equivalence classes. By the same type of argument, this multiplication satisfies

i. it is associative : $([x]\cdot[y])\cdot[z] = [xy]\cdot[z] = [(xy)z] = [x(yz)] = [x]\cdot[yz] = [x]\cdot([y]\cdot[z])$ where the associativity of the product in $\mathbb{Z}$ has been used ;

ii. the equivalent class of 1, represented by 1 in $\{0, 1, \cdots, n-1\}$ is the neutral element since $[x]\cdot[1] = [x1] = [x]$;

iii. it is abelian since $[x]\cdot[y] = [xy] = [yx] = [y]\cdot[x]$, using the commutativity of the product in $\mathbb{Z}$;

iv. it is distributive with respect to the sum $[x]\cdot([y]+[z]) = [x]\cdot[y+z] = [x(y+z)] = [xy+xz] == [xy]+[xz] = [x]\cdot[y]+[x]\cdot[z]$, where the distributivity of the product with respect to the sum in $\mathbb{Z}$ has been used ;

Therefore $\mathbb{Z}_n$ is an abelian ring with -1 being represented by $n-1$ in $\{0, 1, \cdots, n-1\}$.

(f) The multiplication table of $\mathbb{Z}_{21}$ is given below. It is useless to put 0 in it since $0\cdot[x] = 0$ for all $x's$. To simplify it, it has been remarked that $-[x]\cdot[y] = [x]\cdot -[y] = -[x]\cdot[y]$ and that $-[x]\cdot -[y] = [x]\cdot[y]$. Thus it is useless to give the column and the lines corresponding to $-[x]$. On the other hand the representatives of $-1, -2, \cdots, -10$ are respectively $20, 19, \cdots, 11$. Thus it is sufficient to represent only the numbers $1, 2, \cdots, 10$. At last, commutativity implies that the table is symmetric with repect to the main diagonal : for this reason, the lower part of the table below has not been filled.

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	−9	−7	−5	−3	−1
3		9	−9	−6	−3	0	3	6	9
4			−5	−1	3	7	−10	−6	−2
5				4	9	−7	−2	3	8
6					−6	0	6	−9	−3
7						7	−7	0	7
8							1	9	−4
9								−3	6
10									−5

- Multiplication table for $\mathbb{Z}_{21}$ -

Remark : this table shows that $\mathbb{Z}_{21}$ has divisors of zero, such as $\pm 3, \pm 6, \pm 9, \pm 7$.

(g) The list of invertible elements of $\mathbb{Z}_{21}$ can be read on the previous table :

$$1,\ 2,\ 4,\ 8,\ -5,\ -10,\ -1,\ -2,\ -4,\ -8,\ 5,\ 10\,.$$

These are all numbers co-prime to 21 (with no common divisor with 21, namely that are not divisible by 3 or 7). It is to be remarked that $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = -5$, $2^5 = -10$, $2^6 = 1$ so that this group is made of numbers of the form $\pm 2^k$

with $0 \leq k \leq 5$. In particular the map $(\sigma, k) \in \{+1, -1\} \times \mathbb{Z}_6 \mapsto \sigma 2^k \in \mathbb{Z}_{21}^*$ is a group isomorphism.

The solutions of the equation $x^2 = 1 \pmod{21}$ can be read on the diagonal of the multiplication table, namely $x = \pm 1, \pm 8$.

4. (a) If $a = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ and $b = \prod_{p \in \mathcal{P}} p^{\beta_p}$ are the prime decompositions of a and b respectively, then $\gcd(a,b) = \prod_{p \in \mathcal{P}} p^{\gamma_p}$ where $\gamma_p = \min\{\alpha_p, \beta_p\}$ for all p's.

   (b) Let s be the smallest positive (non zero) integer of the form $ax + by$ for $x, y \in \mathbb{Z}$.

   (i) Then (*cf.* (1.a)), $\gcd(a,b)$ divides both a and b and thus it divides s.

   (ii) On the other hand, if $s > a$ then $1 \leq s - a = a(x-1) + by$ is smaller than s and is also of the form $ax' + by'$. This is impossible since s is the smallest such number. Hence $1 \leq s \leq a$. Then the euclidean division of a by s gives $a = ks + r$ for some $k \geq 1$ and $0 \leq r \leq s - 1$. Then $r = a(1 - kx) - by$ is of the form $ax' + by'$, so that, since $0 \leq r < s$ it must vanish. Hence s divides a. The same argument shows that it also divided b. Thus s is a common divisor of a, b and therefore s divides $\gcd(a,b)$.

   Since the relation $a|b$ is an order, it follows from (i) and (ii) that $s = \gcd(a,b)$. As a consequence

   Theorem 1 (Bezout) *$a, b \in \mathbb{N}_*$ are co-prime if and only if there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$*

   Proof : For if a and b are co-prime, $\gcd(a,b) = 1$ and, from the previous argument, there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Conversely, if such a pair x, y exists, 1 is the smallest nonzero positive integer of the from $ax + by$, so that the previous argument shows that $1 = \gcd(a,b)$ which means that a and b are co-prime. □

   (c) If c divides both a and b, then it divides $ax + by$ for any $x, y \in \mathbb{Z}$ (*cf.* question (1.a)). By the previous argument it then divides $\gcd(a,b)$.

5. (a) By Bezout's theorem, x and n are co-prime if and only if there are $m, y \in \mathbb{Z}$ such that $xy + mn = 1$ This is equivalent to $xy = 1 \pmod{n}$, namely to x being invertible *modulo* n.

   (b) The inverse of x in a ring is always unique. For if y and y' are two such inverses, then $xy = yx = 1$ and $xy' = y'x = 1$. Thus $y' = y'(xy) = (y'x)y = y$.

   (c) If p is a prime number, then all non zero elements of $\mathbb{Z}_p$, that is all elements of $\{1, 2, \cdots, p-1\}$, are prime with respect to p, so that there are all invertible *modulo* p. Thus $\mathbb{Z}_p$ is a finite field (*it is denoted by* $\mathbb{F}_p$).

   (d) If $n > 1$ then $n^2 - 1 = (n-1)(n+1)$ so that $(n+1)(n-1) = -1 \pmod{n^2}$. Hence $n + 1$ is invertible *modulo* n^2 and its inverse is the class *modulo* n^2 of $-(n-1)$.

   Second Proof[3] *: using Bezout's theorem,* $1 = (n+1) \cdot 1 + (-1) \cdot n$ *implies that n and $n+1$ are co-prime. Thus $n+1$ is co-prime to n^2 and is therefore invertible modulo n^2*

6. Let $a, b \in \mathbb{N}_*$. If $a = b$ then $\gcd(a,b) = a = b$ so that there is nothing to compute. Therefore one can assume $a > b$ for otherwise it is enough to change the names of a and b.

[3] Due to Drew Roos

(a) Let then r be the rest of the euclidean division of a by b, namely $a = kb + r$ with $0 \leq r \leq b-1$. Since $r = a - kb$ it follows from (1.a) that $\gcd(a,b)$ divides r. Thus it divides both b and r so that, thanks to (4.c) above, $\gcd(a,b) | \gcd(b,r)$. Conversely, since $a = kb + r$, $\gcd(b,r)$ divides also a so that, by (4.c) again, $\gcd(b,r) | \gcd(a,b)$. Hence $\gcd(a,b) = \gcd(b,r)$. If $r = 0$ then $\gcd(a,b) = b$.

(b) If $r \neq 0$, then $1 \leq r \leq b-1$. Then we set $r_{-1} = a$, $r_0 = b$, $r_1 = r$. Let the sequence $r_{-1} > r_0 > r_1 > \cdots > r_j > 0$ be defined so that $\gcd(r_{i-1}, r_i) = \gcd(a,b)$ for $i = 0, 1, \cdots, j$. Then let r_{j+1} be the rest of the division of r_{j-1} by r_j. The previous argument shows that either $r_{j+1} = 0$, and then $\gcd(a,b) = r_j$, or $0 < r_{j+1} < r_j$ and, thanks to (6a), $\gcd(r_j, r_{j+1}) = \gcd(a,b)$. Since all the r_j's are integers, this process must terminate after a finite number of steps. If m is the number of such steps, $\gcd(a,b) = r_m$.

(c) As an example, let us compute $\gcd(2002, 1946)$. Dividing 2002 by 1946 gives

$$r_{-1} = 2002,\ r_0 = 1946, \qquad 2002 = 1946 \times 1 + 56, \qquad \Rightarrow \qquad r_1 = 56\,.$$

$$1946 = 56 \times 34 + 42, \qquad \Rightarrow \qquad r_2 = 42\,.$$

$$56 = 42 \times 1 + 14, \qquad \Rightarrow \qquad r_3 = 14\,.$$

$$42 = 14 \times 3, \qquad \Rightarrow \qquad \gcd(2002, 1946) = 14\,.$$

This result can be checked : $2002 = 143 \times 14$ whereas $1946 = 139 \times 14$. Then $143 = 11 \times 13$ while 139 is a prime number. (*This because* 139 *is not divisible by* $2, 3, 5, 7, 11$, *as can be checked directly, and therefore, since* $11 \times 13 = 143 > 139$, *there is no need to check whether it is divisible by other primes. Hence* 14 *is indeed the* $\gcd(2002, 1946)$.)

(d) The sequence $a = r_{-1} > b = r_0 > r_1 > \cdots > r_m$ satisfies $r_i/2 \geq r_{i+2}$ for $i = -1, 0, \cdots, m-2$. For indeed, either $r_{i+1} \leq r_i/2$, then $r_{i+2} < r_{i+1} \leq r_i/2$, or $r_{i+1} > r_i/2$, then $1 \leq r_i/r_{i+1} < 2$. In the latter case, the euclidean division of r_i by r_{i+1} gives $r_i = r_{i+1} + r_{i+2} > r_i/2 + r_{i+2}$, leading to $0 \leq r_{i+2} < r_i/2$.

(e) It follows from the previous result that $r_m < r_{m-2l}/2^l$ for all l such that $m - 2l \geq -1$. Then if m is even, choose $l = m/2$ so that $r_m < b/2^{m/2} < a/2^{m/2}$. If m is odd, choose $l = (m+1)/2$ leading to $r_m < a/2^{(m+1)/2} < a/2^{m/2}$. In both cases

$$m \ < \ 2 \ln_2(a) \ \leq \ 2L\,.$$

Therefore the computer time required for running this algorithm is $O(L^3)$, since each step of the Euclide algorithm requires $O(L^2)$ elementary operations.

(f) To get the pair $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a,b)$ it is enough to start at the end of the Euclid algorithm and run it backward. Let us treat first the previous example in (6c) :

$$14 = 56 - 42 \times 1,$$

$$42 = 1946 - 56 \times 34, \qquad \Rightarrow \qquad 14 = -1946 \times 1 + 56 \times 35$$

$$56 = 2002 - 1946 \times 1, \qquad \Rightarrow \qquad 14 = -1946 \times 36 + 2002 \times 35$$

In the general case, the recursion goes as follows :

$$r_{-1} \;=\; a, \qquad r_0 \;=\; b, \qquad r_j \;=\; r_{j+1} \times k_{j+1} + r_{j+2}\,,$$

where all numbers are in $\mathbb{N}_*$ and $0 < r_{j+2} < r_{j+1}$, as long as $j \leq m-2$. The process terminates when $j = m-1$ for which $r_{m-1} = k_m r_m$ (which can be interpreted as saying that $r_{m+1} = 0$). Then $r_m = \gcd(a, b)$. This can be written in matrix form as follows

$$\begin{bmatrix} r_j \\ r_{j+1} \end{bmatrix} = \begin{bmatrix} k_{j+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_{j+1} \\ r_{j+2} \end{bmatrix},$$

leading to

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} k_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} k_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} k_m & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \gcd(a,b) \\ 0 \end{bmatrix}.$$

Since all matrix are invertible (their determinant is -1), and since

$$\begin{bmatrix} k & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & -k \end{bmatrix},$$

it follows that

$$\begin{bmatrix} \gcd(a,b) \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -k_m \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -k_0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x & y \\ y' & x' \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \tag{1}$$

Thus $\gcd(a, b) = ax + by$ while $ay' + bx' = 0$. Algorithmically, the product of these $m + 1$ matrices can be done recursively. For indeed, setting, for $0 \leq j \leq m$

$$(-1)^j \begin{bmatrix} -p'_j & q'_j \\ p_j & -q_j \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -k_j \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -k_0 \end{bmatrix},$$

it follows, by recursion that

$$\begin{aligned} &p_{-1} = 0,\; q_{-1} = 1,\; p_0 = 1,\; q_0 = k_0, && p'_j = p_{j-1}\,,\; q'_j \;=\; q_{j-1}\,, \\ &p_{j+1} \;=\; k_{j+1}p_j + p_{j-1}\,, && q_{j+1} \;=\; k_{j+1}q_j + q_{j-1}\,. \end{aligned}$$

Therefore, starting from $p_{-1} = 0,\; q_{-1} = 1,\; p_0 = 1,\; q_0 = k_0 1$, at each step of the Euclid algorithm, the computation of k_j gives $p_j \geq 0$ and $q_j \geq 0$. This leads to storing $p_j, q_j, r_j, p_{j-1}, q_{j-1}, r_{j-1}$ in a memory, while $O(L^2)$ elementary operations are required at each step. Since $m = O(L)$, the algorithm requires also $O(L^3)$ elementary operations. The algorithm ends whenever $r_{m+1} = 0$ leading to $x = (-1)^{m-1}p_{m-1}$, $y = (-1)^m q_{m-1}$, $y' = (-1)^m p_m$, $x' = (-1)^{m-1}q_m$.
It is worth remarking that the determinant of the product of the first $j + 1$ matrices is $(-)^{j+1} = (-1)^{j-1}$ so that

$$q_j p_{j-1} - q_{j-1} p_j \;=\; (-1)^{j-1}\,,$$

showing that q_j and p_j are co-prime. In particular, eq. (1) leads to $ap_m - bq_m = 0$, namely $a/b = q_m/p_m$. Since the last fraction is irreducible, it follows that $a = q_m s$, $b = p_m s$ for $s = \gcd(a, b)$. This is the interpretation of the last two elements of the product of $m + 1$ matrices.

(g) If a and n are co-prime, the previous algorithm produces $x, y \in \mathbb{Z}$ such that $1 = \gcd(a, n) = ax + ny$. In particular $ax = 1 \,(\mathrm{mod}\, n)$, showing that x is the inverse of a *modulo* n.

7. *The Chinese remainder theorem* :

   (a) Let $M = m_1 m_2 \cdots m_k$ and let $M_i = M/m_i$. Then, because the m_j's are mutually co-prime, M_i and m_i are co-prime. Therefore, M_i is invertible *modulo* m_i. Let then $1 \leq N_i < m_i$ be the inverse of M_i *modulo* m_i. Then, if $j \neq i$, $M_j N_j = 0 \,(\mathrm{mod}\, m_i)$, because m_i is a divisor of M_j. On the other hand, $M_i N_i = 1 \,(\bmod\, m_i)$. Therefore the number $x = \sum_{i=1}^k a_i M_i N_i$ is a solution of the Chinese remainder equation :

$$x = \sum_{i=1}^{k} a_i M_i N_i \qquad \Rightarrow \qquad x = a_i \,(\bmod\, m_i)\,.$$

(b) Let x, y be two such solutions. Then $x - y = l_1 m_1 = l_2 m_2 = \cdots = l_k m_k$ for some $l_j \in \mathbb{Z}$. Since m_1 and m_2 are co-prime, it follows that m_2 is a divisor of l_1 so that $x - y = r_2 m_1 m_2$ for some $r_2 \in \mathbb{Z}$. By recursion, if it has been proved that $x - y = r_j m_1 m_2 \cdots m_j$ for some $r_j \in \mathbb{Z}$, then $x - y = l_{j+1} m_{j+1}$ implies that m_{j+1} aldo divides r_j because it does not divides $m_1 m_2 \cdots m_j$. Thus $r_j = r_{j+1} m_{j+1}$ for some $r_{j+1} \in \mathbb{Z}$. Hence, for $j = k$ this gives $x - y = rM$, namely $x - y = 0 \,(\bmod\, M)$.

8. The *Euler φ-function* gives, for $n \in \mathbb{N}$, the number $\varphi(n)$ of positive integers co-prime to n. Therefore, $\varphi(1) = 1$ and, if $n > 1$, $\varphi(n)$ *is nothing but the number of invertible elements of* $\mathbb{Z}_n$.

(a) If $n > 1$, the number of invertible elements in $\mathbb{Z}_n$ is smaller than or equal to $n - 1$. Thus $\varphi(n) < n$.

(b) If $p > 1$ is a prime number, all non zero elements of $\mathbb{F}_p = \mathbb{Z}_p$ are invertible, that is

$$p \in \mathcal{P} \qquad \Rightarrow \qquad \varphi(p) = p - 1\,.$$

(c) In the ring $\mathbb{Z}_{p^\alpha}$, the elements that are not co-prime to p^α are the multiple of p. There are $p^{\alpha-1}$ such elements. Therefore

$$p \in \mathcal{P} \qquad \Rightarrow \qquad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)\,.$$

(d) Let $a, b \in \mathbb{N}_*$ be co-prime. If x is co-prime to ab, it must be co-prime to a and to b. Therefore there are invertible elements $x_a \in \mathbb{Z}_a$ and $x_b \in \mathbb{Z}_b$ such that $x = x_a \,(\bmod\ a)$ and $x = x_b \,(\bmod\ b)$. This pair is unique. Conversely if x is not co-prime to ab, at least one of the divisor of either a or b divides x. Therefore either x_a or x_b is not invertible. On the other hand given a pair $(x_a, x_b) \in \mathbb{Z}_a \times \mathbb{Z}_b$ of invertible elements, the Chinese remainder theorem shows that there is a unique $x \in \mathbb{Z}_{ab}$ satisfying $x = x_a \,(\bmod\, a)$ and $x = x_b \,(\bmod\, b)$. By the previous argument, x is invertible *modulo ab*. Therefore there is a bijection between the set of invertible elements in $\mathbb{Z}_{ab}$ and the set of pairs $(x_a, x_b) \in \mathbb{Z}_a \times \mathbb{Z}_b$ of invertible elements. Hence the number of invertible elements of $\mathbb{Z}_{ab}$ is the product of the number of invertible elements of $\mathbb{Z}_a$ and of $\mathbb{Z}_b$. This shows that $\varphi(ab) = \varphi(a)\varphi(b)$.

(e) *Erratum : in the original problem the relation should be read*

$$n = \sum_{d; d|n} \varphi(d)\,.$$

Let p be a prime number. If $\alpha > 0$, all divisors of p^α are of the form p^β for $0 \le \beta \le \alpha$. For $\beta = 0$, $\varphi(p^0) = 1$. Thus, thanks to (8c),

$$\sum_{d;d|p^\alpha} \varphi(d) \;=\; 1+\sum_{\beta=1}^{\alpha} \varphi(p^\beta) \;=\; 1+(p-1)(1+p+\cdots+p^{\alpha-1}) \;=\; 1+p^\alpha-1 \;=\; p^\alpha\,.$$

Let $n>1$ have the prime factorization $n=\prod_{p\in\mathcal{P}} p^{\alpha_p}$. Any divisor of n is a unique product of the form $d=\prod_{p\in\mathcal{P}} p^{\beta_p}$ with $0\leq\beta_p\leq\alpha_p$. Thus $\varphi(d)=\prod_{p\in\mathcal{P}}\varphi(p^{\beta_p})$. Hence, using the previous result,

$$\sum_{d;d|n} \varphi(d) \;=\; \sum_{0\leq\beta_p\leq\alpha_p;\forall p}\; \prod_{p\in\mathcal{P}} \varphi(p^{\beta_p}) \;=\; \prod_{p\in\mathcal{P}}\sum_{\beta_p=0}^{\alpha_p} \varphi(p^{\beta_p}) \;=\; \prod_{p\in\mathcal{P}} p^{\alpha_p} \;=\; n\,.$$

9. Let n be a positive integer and let $1<x<n-1$ be a solution of $x^2=1$ (mod$n$).
   (a) By definition, $x\neq 1\,(\mathrm{mod}\,n)$, because $1<x<n-1$. Since $x\neq n-1$, $x\neq -1\,(\mathrm{mod}\,n)$ as well.
   (b) The equation $x^2=1$ (mod$n$) can be written as $(x-1)(x+1)=0$ (mod$n$), namely either $(x-1)$ or $(x+1)$ has a non trivial common divisor with n. Thus one of the two $\gcd(x\pm 1,n)$ is a non trivial factor of n.
   (c) Using the Euclid algorithm, computing $\gcd(x\pm 1,n)$ requires $O(L^3)$ elementary operations, whenever L is the minimal number of binary digits required to express n.
10. Let $n=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ be a factorized integer. Let $x\in\{2,\cdots,n-2\}$ be chosen at random (namely with uniform probability) among the integers co-prime to n. Then let r be the order of x, namely r is the smallest non zero positive integer such that $x^r=1\,(\mathrm{mod}\,n)$.
   Let G_x be the set of $r\in\mathbb{Z}$ such that $x^r=1\,(\mathrm{mod}\,n)$. G_x is not empty nor reduced to $\{0\}$. This is because the sequence $\{1,x,x^2.\cdots,x^l,\cdots\}$ is contained in the group of invertible elements of $\mathbb{Z}_n$ which is finite : thus there are at least two integers $s\neq t$ such that $x^t=x^s\,(\mathrm{mod}\,n)$; since x is invertible $(\mathrm{mod}\,n)$, it follows that $x^{t-s}=1\,(\mathrm{mod}\,n)$. Thus $0\neq t-s\in G_x$. If $r,r'\in G_x$ then $r+r'\in G_x$ and $-r\in G_x$, showing that G_x is a subgroup of $\mathbb{Z}$. Therefore there is $r>0$ such that $G_x=r\mathbb{Z}$ and r is precisely the order of x.
   (a) The question is meaningful only if $n>2$, in which case $-1\neq 1\,(\mathrm{mod}\,n)$. Since x is any invertible element of $\mathbb{Z}_n$ not equal to ±1, there are $\varphi(n)-2$ such numbers. Therefore the probability of choosing x is $1/(\varphi(n)-2)$.
   (b) *Erratum : the answer to this question requires more steps than just a few lines answers. Three important results are needed*
      i. *the* little Fermat theorem *which asserts that if p is prime and $a\in\mathbb{N}$ then $a^p=a\,(\mathrm{mod}\,p)$;*
      ii. *the* Euler theorem, *generalizing the little Fermat one, namely if a and n are co-prime, then $a^{\varphi(n)}=1\,(\mathrm{mod}\,n)$;*
      iii. *if p is an odd prime, and if $\alpha>0$, then the group $\mathbb{Z}_{p^\alpha}^*$ of invertible elements of $\mathbb{Z}_{p^\alpha}$ is cyclic, namely there is $g\in\mathbb{Z}_{p^\alpha}^*$ such that $\{1,g,g^2,\cdots,g^{r-1}\}=\mathbb{Z}_{p^\alpha}^*$ for some $r>1$ (g is called a* generator*); such an r is necessarily the number of invertible elements, so that $r=\varphi(p^\alpha)$.*

   The proofs of the results (10(b)i) & (10(b)ii) can be found below in Appendix 1. The proof of (10(b)iii) is more difficult and can be found in books of number theory.

By the Euler theorem, since x is co-prime to n, $x^{\varphi(n)} = 1 \,(\mathrm{mod}\, n)$. Therefore $\varphi(n) \in G_x$ namely, it is a multiple of r. If now p is an odd prime, let $d \geq 1$ be the largest integer such that 2^d divides $p-1$ (*for instance* $p = 17$ *gives* $p - 1 = 16 = 2^4$). Thus d is also the largest integer such that 2^d divides $\varphi(p^\alpha)$.

We claim that *a randomly chosen element* $x \in \mathbb{Z}^*_{p^\alpha}$ *has an order* r *that is divisible by* 2^d *with probability exactly* $1/2$.

For indeed, by (10(b)iii) above, there is a generator g of the group $\mathbb{Z}^*_{p^\alpha}$. Thus $x = g^k$ for some $0 \leq k \leq \varphi(p^\alpha) - 1$. If r is its order, then $g^{kr} = 1 \,(\mathrm{mod}\, p^\alpha)$ so that $kr \in G_x$. Since the order of g is $\varphi(p^\alpha)$, it follows that $\varphi(p^\alpha)$ divides kr. If k is odd, then automatically 2^d divides r. If k is even, then

$$x^{\varphi(p^\alpha)/2} \;=\; g^{k\varphi(p^\alpha)/2} \;=\; \left(g^{\varphi(p^\alpha)}\right)^{k/2} \;=\; 1^{k/2} = 1 \,(\mathrm{mod}\, p^\alpha)\,.$$

In particular $\varphi(p^\alpha)/2 \in G_x$ so that r divides $\varphi(p^\alpha)/2$. Hence, 2^d cannot divide r. Thus for $x = g^k$ with k odd, 2^d divides r, whereas for $x = g^k$ with k even, 2^d does not divide r. This shows that exactly half of the x's have their order divisible by 2^d.

Let now $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ be an odd positive integer. Let x be a randomly chosen invertible element of $\mathbb{Z}_n$ and let r be its order. We claim that *with probability larger than or equal to* $1 - 1/2^m$ *r is even and* $x^{r/2} \neq -1 \,(\mathrm{mod}\, n)$.

By the Chinese remainder theorem, any $x \in \mathbb{Z}^*_n$ can be associated with $(x_1, \cdots, x_m) \in \mathbb{Z}^*_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}^*_{p_m^{\alpha_m}}$ in a unique way, such that $x = x_j \,(\bmod\, p_j^{\alpha_j})$. Thus counting the x's is equivalent to counting such x_j's. From the definition of the order r of x, it follows that $x^r = 1 \,(\mathrm{mod}\, n)$ implies $x_j^r = 1 \,(\mathrm{mod}\, p_j^{\alpha_j})$. Thus the order r_j of x_j divides r. As before let d (resp.d_j) be the largest positive integer such that 2^d (resp. 2^{d_j}) divides r (resp. r_j). Then two cases occur for x not satisfying the claim :

(i) either r is odd, in which case each r_j must be odd, so that $d_j = 0 = d$ and r_j is odd for all j's ;

(ii) or r is even and $x^{r/2} = -1 \,(\mathrm{mod}\, n)$; then $x^{r/2} = -1 \,(\mathrm{mod}\, p_j^{\alpha_j})$ for all j's so that $r/2 \notin G_{x_j}$, which means that is not divisible by r_j. Since r_j divides r, the only possibility is that $d_j = d$, for all j's. This occur with probability exactly $1/2$ for each j. Therefore in both cases, all the d_j's are equal to d. By the previous claim above, at most half of the x_j's chosen in $\mathbb{Z}^*_{p_j^{\alpha_j}}$ are divisible by 2^d and not by 2^{d+1}. For either d is the largest integer such that 2^d divides $p_j - 1$, in which case exactly half of the x_j have $d_j = d$, or it is not and at most half of the x_j's have $d_j = d$. Thus altogether, the fraction of the x's for which either r is odd or r is even but $x^{r/2} = -1 \,(\mathrm{mod}\, n)$ is at most $(1/2)^m$.

11. This gives an algorithm to compute the prime number factorization of n.

    (i) if n is even, then return the factor 2 and change n into $n/2$.

    (ii) check whether $n = a^b$ for some $a \leq 2$ and $b \leq 2$ and return a (this can be done by using a special algorithm).

    (iii) choose randomly x between 1 and $n - 1$. If $\gcd(x, n) > 1$ then return the factor $\gcd(x, n)$ and replace n by $n/\gcd(x, n)$.

(iv) Otherwise, use the order finding algorithm to compute the order r of x.
(v) if r is even and $x^{r/2} \neq -1 \,(\mathrm{mod}\, n)$, then compute $\gcd(x^{r/2} \pm 1, n)$ and test which is a non trivial factor. Then return this factor and divides n by this factor. Otherwise, choose another x.
(vi) if everything fails, then n is a prime number.

1 Appendix : two theorems of Arithmetic

In this Section the three results needed in (10b) will be proved.

Theorem 2 (Little Fermat Theorem) *If p is a prime number and $a \in \mathbb{N}$ then $a^p = a \,(\mathrm{mod}\, p)$.*

Proof : (i) first we claim that, if $0 < k < p$ is an integer, then p divides $\begin{pmatrix} p \\ k \end{pmatrix}$. This is because

$$p(p-1)\cdots(p-k+1) \;=\; \begin{pmatrix} p \\ k \end{pmatrix} \, k(k-1)\cdots 1\,.$$

Since $k \geq 1$ the left hand side is divisible by p. Since p is prime and $k < p$ the term $k(k-1)\cdots 1$ is not divisible by p, leading to the conclusion.
(ii) To prove the theorem, we proceed by induction on a. For $a = 1$, the result is obvious. Suppose the theorem is true for a. Then, using the binomial formula :

$$(a+1)^p \;=\; \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} \, a^k\,.$$

All terms corresponding to $k \neq 0, p$ are divisible by p. Thus, using the induction hypothesis, $(a+1)^p = 1 + a^p = 1 + a \,(\mathrm{mod}\, p)$. Hence $a+1$ satisfies also the theorem. $\square$

Theorem 3 (Euler) *If a and n are co-prime integers, then $a^{\varphi(n)} = 1 \,(\mathrm{mod}\, n)$.*

Proof : (i) Let p be a prime number. By induction on α the theorem is true for $n = p^\alpha$. For indeed, if $\alpha = 1$, this is the little Fermat theorem 2. If, by induction, the result holds for some $\alpha \geq 1$, then

$$a^{\varphi(p^\alpha)} = 1 + kp^\alpha\,,$$

for some $k \in \mathbb{Z}$. Thus, using (8c),

$$\begin{aligned} a^{\varphi(p^{\alpha+1})} &= a^{p^\alpha(p-1)} \\ &= a^{p\varphi(p^\alpha)} \\ &= (1+kp^\alpha)^p \\ &= 1 + \sum_{j=1}^{p} \begin{pmatrix} p \\ k \end{pmatrix} \, k^j p^{j\alpha}\,. \end{aligned}$$

Using the proof of Theorem 2, all terms in the last sum are divisible by $p^{\alpha+1}$, so that

$$a^{\varphi(p^{\alpha+1})} \;=\; 1 \,(\mathrm{mod}\, p^{\alpha+1})\,.$$

$\square$