Mathematics 4: Number Theory Problem Sheet 3

Workshop 26 Oct 2012

The aim of this workshop is to show that Carmichael numbers are squarefree and have at least 3 distinct prime factors.

(1) (Warm-up question.) Show that $n > 1$ is prime iff $a^{n-1} \equiv 1 \pmod{n}$ for $1 \leq a \leq n-1$.

`If` n `is prime, then the result is true by Fermat's Theorem. If` n `is composite, then, for` $a = p$, `a prime factor of` n, `the equation` $p^{n-1} + kn = 1$ `has no solution, since the LHS is divisible by` p. `So result is true iff` n `prime.`

Recall that a positive integer is said to be *squarefree* if it is not divisible by the square of any prime number.

Recall too that a *Carmichael number* is a composite number n with the property that for every integer a coprime to n we have $a^{n-1} \equiv 1 \pmod{n}$.

(2) *Proving that Carmichael numbers are squarefree.*

(a) Show that a given nonsquarefree number n can be written in the form $n = p^\ell N$ for some prime p and integers N and ℓ with $\ell \geq 2$ and $\gcd(p, N) = 1$.

(b) Show that $(1 + pN)^{n-1} \not\equiv 1 \pmod{p^2}$.

(c) Deduce that Carmichael numbers are squarefree.

`(a) Take a prime` p `such that` $p^2 \mid n$. `Then` $p^\ell \| n$ `for some` $\ell \geq 2$. `So` $n = p^\ell N$ `say, where` $N = n/p^\ell$ `is coprime to` p.

`(b) Now` $(1+pN)^{n-1} \equiv 1 + pN(n-1) \pmod{p^2} \equiv 1 - pN \pmod{p^2} \not\equiv 1 \pmod{p^2}$, `by the Binomial Theorem and because` $p^2 \mid n$ `and` $\gcd(N, p) = 1$.

`(c) Now take` $a = 1 + pN$. `Then` $a^{n-1} \not\equiv 1 \pmod{p^2}$ `by (b), so` $a^{n-1} \not\equiv 1 \pmod{n}$. `Hence, as` $\gcd(a, n) = 1$, n `is not a Carmichael number.`

---

(3) *Proving that Carmichael numbers have at least 3 distinct prime factors.*

(a) Let p and q be distinct primes. Prove that if $\gcd(a, pq) = 1$ then $a^{\mathrm{lcm}(p-1,q-1)} \equiv 1 \pmod{pq}$.

(b) Now let g be a primitive root $\pmod p$ and h be a primitive root $\pmod q$. Using g and h, apply the Chinese Remainder Theorem to specify an integer a whose order $\pmod{pq}$ is (exactly) $\operatorname{lcm}(p-1, q-1)$.
(c) Now suppose that p is the larger of the primes p and q.
Calculate $pq - 1 \pmod{p-1} \in \{0, 1, \ldots, p-2\}$.
Deduce that $p - 1 \nmid pq - 1$.
(d) Use the above to show that there is an a with $\gcd(a, pq) = 1$ and $a^{pq-1} \not\equiv 1 \pmod{pq}$.
(e) Deduce from the above that a Carmichael number must have at least 3 distinct prime factors.

(a) By Fermat's Theorem we have $a^{p-1} \equiv 1 \pmod p$ and $a^{q-1} \equiv 1 \pmod q$, so that, taking appropriate powers, $a^{\operatorname{lcm}(p-1,q-1)} \equiv 1 \pmod p$ and $a^{\operatorname{lcm}(p-1,q-1)} \equiv 1 \pmod q$. Hence $a^{\operatorname{lcm}(p-1,q-1)} \equiv 1 \pmod{pq}$.
(b): We simply choose a so that $a \equiv g \pmod p$ and $a \equiv h \pmod q$. This is possible, by CRT. Since g has order $p-1$ modulo p and h has order $q-1$ modulo q, we have that a has order $p-1$ modulo p and order $q-1$ modulo q. Hence a has order $\operatorname{lcm}(p-1, q-1)$ modulo pq.
(c): Now $pq - 1 = (p-1)q + q - 1 \equiv q - 1 \pmod{p-1} \not\equiv 0 \pmod{p-1}$, as $0 < q - 1 < p - 1$. Hence $p - 1 \nmid pq - 1$.
(d): From (b) there is an a whose order $\pmod{pq}$ is $\operatorname{lcm}(p-1, q-1)$, so that if $\gcd(a, p) = 1$ then from (a) we have that $a^k \equiv 1 \pmod{pq}$ iff k is a multiple of $\operatorname{lcm}(p-1, q-1)$. But $pq-1$ is not a multiple of $\operatorname{lcm}(p-1, q-1)$, since $q - 1 \nmid pq - 1$. So $a^{pq-1} \not\equiv 1 \pmod{pq}$.
(e):
Now the number a in (d) is clearly coprime to both p and q, i.e., $\gcd(a, pq) = 1$. Hence, from (d), pq is not a Carmichael number. As Carmichael numbers are not prime and are not divisible by the square of any prime, they must have at least 3 prime factors.

---

(4) (Cool-down question.) Suppose that $a, k, \ell, m, n \in \mathbb{N}$ with $a^k \equiv 1 \pmod m$ and $a^\ell \equiv 1 \pmod n$. Prove that
(a) $a^{\operatorname{lcm}(k,\ell)} \equiv 1 \pmod{\operatorname{lcm}(m, n)}$;
(b) $a^{\gcd(k,\ell)} \equiv 1 \pmod{\gcd(m, n)}$.

(a) Let $kk' = \operatorname{lcm}(k, \ell)$. Then $a^k - 1$ divides $a^{kk'} - 1 = a^{\operatorname{lcm}(k,\ell)} - 1$, so that $a^{\operatorname{lcm}}(k, \ell) \equiv 1 \pmod m$. Similarly, $a^{\operatorname{lcm}(k,\ell)} \equiv 1 \pmod n$. Hence $a^{\operatorname{lcm}(k,\ell)} - 1$ is divisible by both m and n. Writing $m = \prod_p p^{e_p}$ and $n = \prod_p p^{f_p}$, we see that, for each p prime, $a^{\operatorname{lcm}(k,\ell)} - 1$ is divisible by $p^{\max(e_p, f_p)}$, and so is divisible by $\prod_p p^{\max(e_p, f_p)} = \operatorname{lcm}(m, n)$. So $a^{\operatorname{lcm}(k,\ell)} \equiv 1 \pmod{\operatorname{lcm}(m, n)}$.

(b) From $a^k \equiv 1 \pmod m$ and $a^\ell \equiv 1 \pmod n$ and the fact that $G = \gcd(m,n)$ divides both m and n we have $a^k \equiv 1 \pmod G$ and $a^\ell \equiv 1 \pmod G$. Next, by the Extended Euclidean Algorithm we can find integers k_1 and ℓ_1 such that $kk_1 + \ell\ell_1 = \gcd(k,\ell)$. Hence

$$a^{\gcd(k,\ell)} = a^{kk_1+\ell\ell_1} = (a^k)^{k_1} \cdot (a^\ell)^{\ell_1} \equiv 1^{k_1} \cdot 1^{\ell_1} \equiv 1 \pmod G.$$

Handin: due Friday, week 7, 2 Nov, before 12.10 lecture. Please hand it in at the lecture

The squarefree part of n

You are expected to write clearly and legibly, giving thought to the presentation of your answer as a document written in mathematical English.

(5) (a) Show that every positive integer n can be written uniquely in the form $n = n_1 n_2^2$, where n_1 is squarefree.
Let us denote n_1 by $g(n)$, the *squarefree part of n*.
(b) Prove that $g(n)$ is a multiplicative function.
(c) Find the Euler product for $D_g(s)$.
(d) Prove that $D_g(s) = \zeta(2s)\zeta(s-1)/\zeta(2s-2)$.

(a) From $p^{2k+1} = p \cdot (p^k)^2$ and $p^{2k} = 1 \cdot (p^k)^2$ we see that we can take n_1 to be the product of primes that divide n to an odd power, as then n_1 is squarefree and n/n_1 is a square, $= n_2^2$ say. [2 marks]
(b) For $\gcd(m,n) = 1$, $g(m)g(n) = m_1 n_1$ with $\gcd(m_1, n_1) = 1$, so that $mn = m_1 n_1 (m_2 n_2)^2$, with $m_1 n_1$ squarefree, giving $g(mn) = m_1 n_1 = g(m)g(n)$. [2 marks]

(c) Now $g(p^{2k+1}) = p$, $g(p^{2k}) = 1$ so that

$$\sum_{k=1}^{\infty} \frac{g(p^k)}{p^{ks}} = \sum_{k \text{ odd}} \frac{p}{p^{ks}} + \sum_{k \text{ even}} \frac{1}{p^{ks}}$$
$$= (p/p^s + 1)(1 + 1/p^{2s} + 1/p^{4s} + \dots)$$
$$= (1 + 1/p^{s-1})/(1 - 1/p^{2s}).$$

Hence $D_g(s) = \prod_p (1 + 1/p^{s-1})/(1 - 1/p^{2s})$. [3 marks]
(d) Then

$$D_g(s) = \prod_p (1 + 1/p^{s-1})/(1 - 1/p^{2s})$$
$$= \prod_p (1 - 1/p^{2s-2})/((1 - 1/p^{2s})(1 - 1/p^{s-1}))$$
$$= \zeta(2s)\zeta(s-1)/\zeta(2s-2).$$

[3 marks]

Problems on congruences

(6) Let $m_1, \dots, m_n$ be pairwise relatively prime. Show that as x runs through the integers $x = 1, 2, 3, \dots, m_1 m_2 \cdots m_n$, the n-tuples ($x \mod m_1, x \mod m_2, \dots, x \mod m_n$) run through all n-tuples in $\prod_{i=1}^{n} \{0, 1, \dots, m_i - 1\}$.

If for $x, x' \in \{1, 2, 3, \dots, m_1 m_2 \cdots m_n\}$ the n-tuples

$$(x \mod m_1, x \mod m_2, \dots, x \mod m_n)$$

and

$$(x' \mod m_1, x' \mod m_2, \dots, x' \mod m_n)$$

were equal, then the n-tuple $(x - x' \mod m_1, x - x' \mod m_2, \dots, x - x' \mod m_n)$ would be 0, so that $x - x'$ would be divisible by $m_1 m_2 \cdots m_n$. This is impossible as they differ by less than this number. Hence all the n-tuples $(x \mod m_1, x \mod m_2, \dots, x \mod m_n)$ for $x = 1, 2, 3, \dots, m_1 m_2 \cdots m_n$ are different. As there are only $m_1 m_2 \cdots m_n$ of them, they must run through them all.

---

(7) Show that the equation $x^y \equiv 2 \pmod{19}$ has a solution in integers $\{x, y\}$ iff x is congruent to a primitive root mod 19. Deduce that then y is uniquely specified mod 18.

Now (easily checked) 2 is a primitive root $\pmod{19}$, so if x is not a primitive root, then x^y certainly isn't. On the other hand, if x *is* a primitive root, then the powers x^y with $\gcd(y, 18) = 1$ give all primitive roots, including 2. Also, if $\gcd(y, 18) > 1$ then x^y is not a primitive root. As $x^{18} \equiv 1 \pmod{19}$, y is uniquely specified $\pmod{18}$.

---

(8) *Wilson's Theorem.* This states that, for a prime p, we have $(p-1)! \equiv -1 \pmod{p}$.

Prove Wilson's Theorem in (at least!) two different ways.

[Suggestions: (i) Factorize $x^{p-1} - 1$ over $\mathbb{F}_p$. (ii) Try to pair up $a \in \{1, \dots, p-1\}$ with its multiplicative inverse.]

(i) Since, from Fermat's Theorem, $x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-(p-1)) \pmod{p}$, Wilson's Theorem follows on putting $x = 0$.

(ii) For any $a \in \{1, 2, \dots, p-1\}$ there's an $a' \in \{1, 2, \dots, p-1\}$ with $aa' \equiv 1 \pmod{p}$. Further, $a' = a$ iff $a = 1$ or $p - 1$. Hence, in $(p-1)!$, the numbers forming this product can be cancelled in pairs, apart from 1 and $p - 1$. Hence result.

---

(9) (a) Find a primitive root for the prime 23.
(b) How many such primitive roots are there?
(c) Find them all.
(d) Find all the quadratic residues and all the quadratic non-residues $\pmod{23}$.

(a) 5 is one.
(b) $\phi(\phi(23)) = \phi(22) = 10$.
(c) All powers $5^k \pmod{23}$ with $\gcd(k, 22) = 1$, i.e. $5, 10, 20, 17, 11, 21, 19, 15, 7, 14$
(d) The quadratic residues are the even powers of $5 \pmod{23}$, namely $2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1$, while the quadratic nonresidues are the odd powers of $5 \pmod{23}$, namely $5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22$.

---

(10) Solve the equation $x^6 = 7$ in $\mathbb{F}_{19}$, i.e. the equation $x^6 \equiv 7 \pmod{19}$ for $x \in \{0, 1, \dots, 18\}$.

(Solution by standard procedure) Now 2 is a primitive root for 19, and then $2^6 = 64 = 7$ in $\mathbb{F}_{19}$. Putting $x = 2^y$, we need to solve $x^6 = 2^{6y} = 7 = 2^6$ in $\mathbb{F}_{19}$, i.e. $6y \equiv 6 \pmod{18}$. So $y \equiv 1 \pmod{3}$, $y = 1, 4, 7, 10, 13, 16$, $x = 2^y \equiv \pm 2, \pm 3, \pm 5 \pmod{19}$.

---

(11) (a) Let an integer $n > 1$ be given, and let p be its smallest prime factor. Show that there can be at most $p - 1$ consecutive positive integers coprime to n.
(b) Show further that the number $p - 1$ in (a) cannot be decreased, by exhibiting $p - 1$ consecutive positive integers coprime n.
(c) What is $\gcd(p - 1, n)$?
(d) Show that $2^n \not\equiv 1 \pmod{n}$.

(a) Every pth number is divisible by p, which implies the result.
(b) None of $1, 2, 3, \dots, p-1$ has a factor in common with n as all their prime factors are smaller than p, while p is the smallest prime factor of n.
(c) This is 1, as all prime factors of $p - 1$ are less than p, as in (b).
(d) Assume $2^n \equiv 1 \pmod{n}$. As $p \mid n$ we have $2^n \equiv 1 \pmod{p}$ and also (Fermat) $2^{p-1} \equiv 1 \pmod{p}$. Hence $2^{\gcd(p-1,n)} \equiv 1 \pmod{p}$, so by (c) $2^1 \equiv 1 \pmod{p}$, $p \mid 1$, a contradiction.

Problems on arithmetic functions

(12) (a) Let a divisor d of n be given. Among the integers $k = 1, 2, \ldots, n$ show that $\varphi(n/d)$ of them have $\gcd(k, n) = d$.
(b) Deduce that $\sum_{d|n} \varphi(d) = n$.
(c) Deduce that $\varphi(n) = \sum_{d|n} d\mu(n/d)$.

(a) Those k with $\gcd(k, n) = d$ are of the form $k = k'd$ with $k' \le n/d$ and $\gcd(k', n/d) = 1$. So there are $\varphi(n/d)$ of them.
(b) Every $k = 1, \ldots, n$ has $\gcd(k, n) = d$ for some divisor d of n, so number of k's $= n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$.
(c) Comes immediately from Möbius inversion.

---

(13) (a) Prove that $\sum_{d|n} \mu(d) = \Delta(n)$, the 1-detecting function.
(b) Let g be any function $\mathbb{R}_{\ge 0} \to \mathbb{R}$, and put $G(x) = \sum_{n \le x} g(x/n)$, the sum being taken over all positive integers $n \le x$. Prove that if $x \ge 1$ then $g(x) = \sum_{n \le x} \mu(n) G(x/n)$.

(a) Now the function $\sum_{d|n} \mu(d)$ equals 1 for $n = 1$, and is 0 for n a prime power. Also, it is multiplicative, as it is the sum-over-divisors of the multiplicative function μ. Hence it is 0 for all $n > 1$, and hence is $\Delta(n)$.
(b)Now RHS$= \sum_{n \le x} \mu(n) G(x/n) = \sum_{n \le x} \mu(n) \sum_{k \le x/n} g(x/nk)$. Putting $d = nk$ we have that this equals $\sum_{d \le x} g(x/d) \sum_{n|d} \mu(n) = \sum_{d \le x} g(x/d)\Delta(d) = g(x)$ using definition of Δ.

---

(14) (a) For which integers n is $\tau(n)$ odd? Here $\tau(n)$ is the number of (positive) divisors of n.
(b) Prove that $\sum_{k|n} \tau(k)^3 = \left(\sum_{k|n} \tau(k)\right)^2$.
[Note that both sides of the equation are multiplicative functions of n.]

(a) Now p^k has $k+1$ divisors, which is odd for k even. Hence $\tau(n)$ is odd exactly when $n = \prod_p p^{e_p}$ when all e_p are even, i.e., when n is a square.
(b) First prove multiplicitivity of each side. Then take $n = p^{k-1}$. Then LHS$=$ $\tau(1)^3 + \tau(p)^3 + \cdots + \tau(p^{k-1})^3 = 1^3 + 2^3 + \cdots + k^3 = (k(k+1)/2)^2$ (well-known formula). Similarly RHS$= (1 + 2 + \cdots + k)^2 = (k(k+1)/2)^2$, so the result is true for prime powers. Therefore by multiplicitivity, it's true for all n.

---

(15) (a) An arithmetic function $f(n)$ is said to be *strongly multiplicative* if $f(nm) = f(n)f(m)$ for all $n, m \in \mathbb{N}$. Show that a strongly multiplicative function is completely determined by its values at primes.
(b) Show that if $f(n)$ is a strongly multiplicative function then the Euler product of its Dirichlet function $D_f(s)$ is of the form $\prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}$.

(a) For such a function, and $n = p^k \dots q^\ell$, we have $f(n) = f(p^k \dots q^\ell) = f(p)^k \dots f(q)^\ell$, so $f(n)$ is determined by $f(p), \dots, f(q)$.
(b) We have $D_f(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots + \frac{f(p^{ks})}{p^{ks}} + \dots\right) = \prod_p \left(\sum_{k=0}^{\infty} (\frac{f(p)}{p^s})^k\right)$ using total multiplicitivity. Summing this GP gives the result.

---

(16) *Strengthening Euler's Theorem.* Suppose that n factorizes as $n = p_1^{f_1} \cdots p_k^{f_k}$. Show that then, for $\gcd(a, n) = 1$, $a^N = 1 \pmod n$, where

$$N = \operatorname{lcm}(p_1^{f_1} - p_1^{f_1-1}, p_2^{f_2} - p_2^{f_2-1}, \dots, p_k^{f_k} - p_k^{f_k-1}).$$

For which n is this result no stronger than Euler's theorem $a^{\varphi(n)} = 1 \pmod n$?

(17) For two arithmetic functions $A(n)$ and $B(n)$ show that

$$\sum_{d|n} A(d)B(n/d) = \sum_{d|n} A(n/d)B(d).$$

This is just replacing the sum over all divisors d of n with the sum over its 'conjugate divisors' n/d, which are again the set of all divisors of n.

---

(18) (a) Find the Euler product for $D_{|\mu|}(s) = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s}$.
(b) Prove that $D_{|\mu|}(s) = \zeta(s)/\zeta(2s)$.

(a) Now $|\mu(n)| = 1$ if n is squarefree, $= 0$ otherwise. Hence $\sum_{k=1}^{\infty} |\mu(p^k)|/p^{ks} = 1 + 1/p^s$ so, as $|\mu(n)|$ is multiplicative, $D_{|\mu|}(s) = \prod_p (1 + 1/p^s)$.
(b) Follows from $\zeta(s) = \prod_p (1 - 1/p^s)^{-1}$ and $1 + 1/p^s = (1 - 1/p^{2s})/(1 - 1/p^s)$.

---

(19) Let $\omega(n)$ denote the number of prime factors of n. Show that the function $e^{\omega(n)}$ is a multiplicative function.

(20) Let f be any arithmetic function.
(a) Show that $\sum_{n \le x} \sum_{k|n} f(k) = \sum_{n \le x} f(n) \left\lfloor \frac{x}{n} \right\rfloor$.
(b) Now put $F(x) = \sum_{n \le x} f(n)$. Deduce that $\sum_{n \le x} f(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n \le x} F\left(\frac{x}{n}\right)$.

(a) Now $\sum_{n\le x}\sum_{k|n} f(k) = \sum_{k\le x} f(k)\times \#\{n = jk, n\le x\} = \sum_{k\le x} f(k)\left\lfloor \frac{x}{k}\right\rfloor =$ answer except with k instead of n.

(b) We have RHS$= \sum_{n\le x} F\left(\frac{x}{n}\right) = \sum_{n\le x}\sum_{k\le \frac{x}{n}} f(k) = \sum_{k\le x} f(k)\sum_{n\le \frac{x}{k}} 1 = \sum_{k\le x} f(k)\left\lfloor \frac{x}{k}\right\rfloor =$LHS, as required.

---

(21) (a) Prove that for $x\ge 1$ we have $\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor = 1$.
(b) (Harder) Deduce that for all $x\ge 1$ we have

$$\left|\sum_{n\le x}\frac{\mu(n)}{n}\right|\le 1.$$

(a) Apply Q9(a) with $f(n)=\mu(n)$, using the fact that $\sum_{k|n}\mu(k)=\Delta(n)$ ($=1$ for $n=1$, 0 otherwise).

(b) Write $\frac{x}{n}=\left\lfloor\frac{x}{n}\right\rfloor+\delta_n$, where $0\le\delta_n<1$. (Of course δ_n depends on x too.) Then from (a) we get successively

$$\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor = 1$$

$$\sum_{n\le x}\mu(n)(\frac{x}{n}-\delta_n) = 1$$

$$x\sum_{n\le x}\frac{\mu(n)}{n} = 1+\sum_{n\le x}\mu(n)\delta_n.$$

It remains to analyse the RHS of the last equation to verify that it's always at most x in modulus. Since $\mu(2)=\mu(3)=-1$ and $\mu(4)=0$ we see that RHS$\in(-1,1]$ for $1\le x\le 4$. So for $x>4$ we have $|\text{RHS}-v|\le x-4$, where $v\in(-1,1)$. Hence $|\text{RHS}|\le 1+x-4=x-3\le x$. So the RHS is at most x in modulus for all $x\ge 1$.

---

(22) The Dirichlet series $D_f(s)$ of a certain arithmetic function $f(n)$ has Euler product $\prod_p\left(1-\frac{1}{p^s}+\frac{1}{p^{2s}}\right)$.
(a) Show that $f(n)\ne 0$ iff n is "cube-free", and give a precise definition of this term.
(b) Find an explicit description of $f(n)$.
(c) Find the Euler product for $D_{|f|}(s)=\sum_{n=1}^{\infty}\frac{|f(n)|}{n^s}$.
(d) Prove that $D_{|f|}(2s)=D_{|f|}(s)D_f(s)$.

(a) An integer n is said to be *cube-free* if $k^3 \nmid n$ for every integer $k > 1$.

(b) If n is cube-free then $f(n)$ is $(-1)^\ell$, where ℓ is the number of primes p for which $p|n$ but $p^2 \nmid n$. Otherwise $f(n) = 0$.

(c) $D_{|f|}(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}}\right)$.

(d) Here we use the fact that $(1+x+x^2)(1-x+x^2) = 1+x^2+x^4$. Hence

$$\left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}}\right)\left(1 - \frac{1}{p^s} + \frac{1}{p^{2s}}\right) = \left(1 + \frac{1}{p^{2s}} + \frac{1}{p^{4s}}\right),$$

and so $D_{|f|}(2s) = D_{|f|}(s)D_f(s)$.

Problems around primality testing

(23) *Fast exponentiation: Computing a^r by the SX method.*

Let $a \in \mathbb{Z}, r \in \mathbb{N}$. Write r in binary as $r = b_k b_{k-1} \cdots b_1 b_0$, with all $b_i \in \{0, 1\}$. From the binary string $b_k b_{k-1} \cdots b_1 b_0$ produce a string of S's and X's by replacing each 0 by S and each 1 by SX. Now, starting with $A = 1$ and working from left to right, interpret S as $A \to A^2$ (i.e. replace A by A^2), and X as $A \to Aa$ (multiply A by a).

Prove that the result of this algorithm is indeed a^r.

[This algorithm is particularly useful for exponentiation (mod n), but it works for any associative multiplication on any set. Note that the leading S does nothing, so can be omitted.]

(24) Compute 2^{90} (mod 91) by the SX method. What does this tell you about 91?

[Maple: `convert(n,binary);`]

(25) (a) Show that if n is not a pseudoprime to base bb' where $\gcd(b, b') = 1$ then it is not a pseudoprime either to base b or to base b'.

(b) Show that if n is not a pseudoprime to base b^k where $k > 1$ then it is not a pseudoprime to base b.
[Thus it's always enough to use the pseudoprime test with prime bases.]

(c) Repeat (a) and (b) with 'pseudoprime' replaced by 'strong pseudoprime'.

(26) Show that the Carmichael number 561 is not a strong pseudoprime to base 2, but that 2047 is. Show, however, that 2047 is not a strong pseudoprime to base 3.

[Useful Maple: `with(numtheory);?phi,?mod`]

(27) (a) Prove that if $6k + 1, 12k + 1$ and $18k + 1$ are all prime, then their product is a Carmichael number. [Use Q 16]

(b) Show that the first few values of k for which (a) gives Carmichael numbers are $k = 1, 6, 35, 45, \ldots$. What is the next such value of k?
[This is the integer sequence A046025– via "integer sequences", found e.g., by Google]
[Maple `?isprime`]

(a) Suppose $p = 6k+1, q = 12k+1$ and $r = 18k+1$ all prime. Then by Q 16 as $\operatorname{lcm}(p-1, q-1, r-1) = 36k$, we have $a^{36k} \equiv 1 \pmod{pqr}$ for $(a, pqr) = 1$.
But $pqr - 1 = 36k(36k^2 + 11k + 1)$, so $a^{pqr-1} \equiv 1 \pmod{pqr}$ for $(a, pqr) = 1$. Hence pqr is a Carmichael number.
(b) 51. (then 55,56,100,121,195,...)