Løsningsforslag eksamen 2003.

Problem 1 2003: Probably a misprint $g = b$. Applying $\log_b$ to these two congruences one obtain the linear system of congruences:

$$2x + 87 \equiv 53 + 5y + 35 (\bmod 106)$$
$$3x + 18 \equiv 7y + 23 (\bmod 106)$$

which gives that $x = \log_b a = 18$ and $y = \log_b c = 7$.

Problem 2 2003: a) $p - 1 = 2q$ so 5 has order 2, q or $2q$. 5 does not have order two since $5^2 = 25 \not\equiv 1 (\bmod p)$. If $5^q \equiv 1 (\bmod p)$, then 5^q is a quadratic residue modulo p. So let (a/b) denotes the Legendre or Jacobi symbol and the rules in section 5.4.2 can be applied. $(5^q/p) = (5/p)^q = (5/p) = (p/5) = (2/5) = -1$. From this we get that $5^q \not\equiv 1 (\bmod p)$ and therefore 5 is a primitive element modulo p.

b) The same applied to 11 gives that $(11^q/p) = (11/p)^q = (11/p) = -(p/11) = -(10/11) = -(2/11)(5/11) = (5/11) = (11/5) = (1/5) = 1$. Hence $11^q \equiv 1 (\bmod p)$ and 11 is not a primitive element modulo p.

c) There are $\phi(p - 1) = q - 1$ generators, and a total of $p - 3$ elements to choose from so the probability that a random chosen number in the given range is a generator is $(q - 1)/(p - 3)$ which is $1/2$.

Problem 3 2003: a) The order of an element h in a group G is the number of elements in the subgroup of G generated by h, or what is the same, the smallest natural number n such that $h^n = e$ in the group, where e denotes the identity and the group is written as a multiplicative group.

b)We think of the order of 2 in the the multiplicative group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n$.

c) The order of 2 is a divisor of $\phi(n) = 2^{16}(2^{127} - 2) = 2^{17}(2^{126} - 1)$. $\mathbb{Z}_n^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Now $2^{16} \equiv -1 (\bmod p)$ so $2^{32} \equiv 1 (\bmod p)$, and $2^{127} \equiv 1 (\bmod q)$, and since $\gcd(32, 127) = 1$ the order of 2 is $32 \cdot 127 = 4052$.

Problem 4 2002: a) $\mathbb{Z}_n^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^* \simeq Z_{3306} \times Z_{4408} \simeq \mathbb{Z}_6 \times \mathbb{Z}_{551} \times \mathbb{Z}_8 \times \mathbb{Z}_{551}$, Hence knowing these isomorphisms and the residues modulo 24 and 551 determines a d which will work. So I trust the expert.

b) $d = 11131$

Problem 5 2003: a) f has no linear term, and not divisible with any of the listed polynomials, hence f is irreducible.

b) $g = (x^2 + x + 1)^3$ so g is reducible.

Problem 6 2003: $p = f$. Since $\gcd(f, x^{21} - 1) \neq 1$, it follows that f divides $x^{21} - 1$, and x has order 21 in the field.

The recurrence relation is $c_n = c_{n-2} + c_{n-4} + c_{n-5} + c_{n-6}$. Since this recurrence relation has period 21, we get that $c_2 = c_{65} = 0$ $c_3 = c_{66} = 1$, $c_0 = c_{84} = 1$, $c_1 = c_{85} = 0$, $c_4 = c_{109} = 1$ and $c_5 = c_{110} = 1$ (There is a misprint in the last pair.)