(j)

i	0	1	2	3	4	5	6	7	8	9
a_i	159	1	2	1	1	2	4	1	5	1
b_i	159	160	479	639	1118	2875	12618	15493	13550	3532
b_i^2 *mod n*	−230	89	−158	145	−115	61	−227	50	−167	145

$B = \{-1, 2, 5, 23, 29\}$; $b = 639 \cdot 3532$; $c = 5 \cdot 29$; $g.c.d.(b+c, n) = 97$.

(k)

i	0	1	2	3	4	5	6	7	8
a_i	133	1	2	4	2	3	1	2	1
b_i	133	134	401	1738	3877	13369	17246	12115	11488
b_i^2 *mod n*	−184	83	−56	107	−64	161	−77	149	−88

$B = \{-1, 2, 7, 11, 23\}$; $b = 401 \cdot 3877 \cdot 17246 \cdot 11488$; $c = 2^6 \cdot 7 \cdot 11$; $g.c.d.(b+c, n) = 61$.

§ **V.5.**

2. Part 6) is the most time-consuming. Time is bounded by

$$O\left(\sum_{\text{primes } p \le P} \frac{A}{p} \log p \log n\right) = O(A \log n \log P \log\log P).$$

(The question asked only about steps 1–7; the other time-consuming stage for very large n is finding linearly dependent rows modulo 2 in the matrix of exponents corresponding to the B-numbers among the $t^2 - n$.)

3. (a)

t	$t^2 - n$	2	13	17	19	29	37	41	47
1030	14297	–	–	1	–	2	–	–	–
1319	693158	1	–	1	1	1	1	–	–
1370	830297	–	2	3	–	–	–	–	–
1493	1182446	1	–	–	1	2	1	–	–

Rows 1 and 3 are dependent and lead to the factorization $1879 \cdot 557$.