

### Extra Solutions 1

1. (ii)  $(11^2 \cdot 13 \cdot 17^2)^2 = (11^3 \cdot 13^2 \cdot 17) \cdot (11 \cdot 17^3) = (3306^2 - n)(3834^2 - n)$ , which equals  $(3306 \cdot 3834)^2 - n(3306^2 + 3834^2 - n)$ . So  $(3306 \cdot 3834)^2 - (11^2 \cdot 13 \cdot 17^2)^2$  is exactly  $n(3306^2 + 3834^2 - n)$ . Use Euclidean Algorithm to find the gcd of  $n$  and  $3306 \cdot 3834 - 11^2 \cdot 13 \cdot 17^2 = 12220607$ . The sequence of remainders obtained is 1345014, 115481, 74723, 40758, 33965, 6793, 0, and the upshot is that  $n = 6793 \cdot 1601$ .

The least  $a$  such that  $a^2 - n$  is a square is  $\frac{1}{2}(6793 + 1601) = 4197$ . So to factorize  $n$  by Fermat's method one would compute  $a^2 - n$  for all  $a$  from  $\sqrt{n} \approx 3298$  to 4197 before achieving success.

My strategy was to use trial division by small primes on all the values of  $a^2 - n$ , looking for cases where  $a^2 - n$  has only small prime factors. I just used primes up to 20; so I had to go a long way (up to  $3834^2 - n$ ) before I found the relations that enabled me to find a difference of two squares that is divisible  $n$ . It is better to use a larger bound on the size of the prime factors of  $a^2 - n$ : if I had allowed primes up to 100 I would have only had to go as far as  $a = 3350$ .

This method of factorizing was invented in 1981 by J. D. Dixon of Carleton University, Canada.

3. (iii) In view of the earlier parts of the question we only have to prove that if  $p$  is an odd prime number then  $(p-1)! + 1$  is a multiple of  $p$ . Using congruence notation (highly advisable!), we must prove that  $(p-1)! \equiv -1 \pmod{p}$ .

We have seen in lectures that if  $\gcd(a, m) = 1$  then  $a$  has an inverse modulo  $m$ : there is a  $b$  such that  $ab \equiv 1 \pmod{m}$ . Of course this congruence remains valid if  $b$  is replaced by its residue mod  $m$ ; so we can assume that  $1 \leq b \leq m-1$ . In particular, if  $p$  is prime and  $a \in \{1, 2, \dots, p-1\}$  then  $\gcd(a, p) = 1$ , and so there is a  $b \in \{1, 2, \dots, p-1\}$  with  $ab \equiv 1 \pmod{p}$ .

Since the set  $\{1, 2, \dots, p-1\}$  has an even number of elements the above considerations suggest that we can pair up every element of the set with its inverse, and rearrange the product  $1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-1)$  as  $(a_1 b_1)(a_2 b_2) \cdots (a_k b_k)$ , where  $k = \frac{1}{2}(p-1)$  and  $a_i b_i \equiv 1 \pmod{p}$  for each  $i$ . But this would give us  $(p-1)! \equiv 1 \pmod{p}$ , which is wrong. So there had better be an error in the argument.

The "pairing up" idea assumes that each element of  $\{1, 2, \dots, p-1\}$  has a unique inverse in  $\{1, 2, \dots, p-1\}$ , and that the inverse of the inverse of  $a$  is always equal to  $a$ . These are both true (and we should prove them). However, we neglected the possibility that an element might be its own inverse. Note that there had better be an even number of elements that are their own inverses (to go with a certain number of pairs and give us an even number of things in total).

*If  $\gcd(a, p) = 1$  then the inverse of  $a$  modulo  $p$  is unique up to congruence modulo  $p$ .*

*Proof:* Suppose that  $ab \equiv 1 \pmod{p}$  and  $ab' \equiv 1 \pmod{p}$ . Then

$$b \equiv b1 \equiv b(ab') \equiv (ba)b' \equiv 1b' \equiv b' \pmod{p}$$

as required. □

If  $b$  is the inverse of  $a$  modulo  $p$  then  $a$  is the inverse of  $b$  modulo  $p$ .

This is obvious: in both cases the condition is that  $ab$  (which equals  $ba$ ) is congruent to 1 (mod  $p$ ).

If  $a \in \{1, 2, \dots, p-1\}$  is self-inverse modulo  $p$  then  $a = 1$  or  $a = p-1$ .

*Proof:* Suppose that  $a^2 \equiv 1 \pmod{p}$ . Then  $p|(a^2 - 1) = (a-1)(a+1)$ , and by a result proved in lectures this implies (since  $p$  is prime) that either  $p|(a-1)$  or  $p|(a+1)$ . Given that  $a \in \{1, 2, \dots, p-1\}$ , the former alternative can only hold if  $a = 1$  and the latter only if  $a = p-1$ .  $\square$

Note that  $p-1 \equiv -1 \pmod{p}$ , and since  $(\pm 1)^2 = 1$  we conclude that 1 and  $-1$  are indeed self-inverse. Our modified pairing up argument now gives

$$(p-1)! = 1(p-1)(a_1b_1)(a_2b_2) \cdots (a_kb_k) \equiv 1(-1)1^k \equiv -1 \pmod{p}$$

where  $k = \frac{1}{2}(p-3)$  and  $a_i, b_i$  are inverse to one another (and distinct from each other) for all  $i$ .

5. (iii) There was nothing special about 2 in the solutions to Parts (i) and (ii): if  $a = qb+r$  for some integers  $q$  and  $r$  with  $0 \leq r < b$  then  $n^a - 1 = Q(n^b - 1) + n^r - 1$  for some  $Q$  (namely,  $Q = n^r(1 + n^b + n^{2b} + \cdots + n^{(q-1)b})$ ). Since  $0 \leq n^r - 1 < n^b - 1$  this shows that if  $r$  is the residue of  $a$  modulo  $b$  then  $n^r - 1$  is the residue of  $n^a - 1$  modulo  $n^b - 1$ .

The Euclidean Algorithm can be stated as follows. Define  $r_{-2} = a$  and  $r_{-1} = b$ , and then successively for  $r = 0, 1, 2, \dots$ , define  $r_i$  to be the residue of  $r_{i-2}$  modulo  $r_{i-1}$ , stopping when we find  $r_m = 0$ . Then the gcd of  $a$  and  $b$  is  $r_{m-1}$ .

Suppose that the Euclidean Algorithm applied to  $a$  and  $b$  generates the sequence  $r_0, r_1, r_2, \dots, r_m = 0$ . Then, by the result proved in the first paragraph above, the Euclidean Algorithm applied to  $n^a - 1$  and  $n^b - 1$  will generate the sequence  $n^{r_0} - 1, n^{r_1} - 1, n^{r_2} - 1, \dots, n^{r_m} - 1 = 0$ . So  $\gcd(n^a - 1, n^b - 1) = n^d - 1$ , where  $d = r_{m-1} = \gcd(a, b)$ .