Parabola Volume 45, Issue 1 (2009)

Partitions of Primes

Christian Aebi[1] and Grant Cairns[2]

Problem 461 from *Parabola* (1980, issue 2, p. 32) asked: Partition the set $P_n = \{2, 3, 5, \ldots, p_n\}$ of the first n primes into two nonempty disjoint parts A, B and let a, b be their respective products. Is $|a-b|$ always a prime or 1? If not, find the smallest n for which it isn't. The answer (given in *Parabola* 1981, volume 17, issue 1, p. 31–32) is *no*, and the smallest n is 5. Taking $A = \{2, 5, 7, 11\}$ and $B = \{3\}$, one has $a = 770, b = 3$ and $a - b = 767 = 13 \cdot 59$. To see this, the key observation is that the numbers a, b share no common factors. It follows that the prime factors of $a-b$ can't divide either a or b. So the smallest possible prime factor of $a - b$ is p_{n+1}. Armed with this information, it doesn't take long to find the required answer. And this is all done easily by hand; after all, the problem was posed in 1980. We propose a modern variation of this problem.

Problem A Consider all possible partitions of the set P_n of the first n primes into two disjoint parts A, B and let a, b be their respective products[3]. Is the *smallest* of the differences $|a - b|$ always a prime or 1? If not, find the smallest n for which it isn't.

Hints Without loss of generality we may assume that $a > b$. Let k denote the smallest of the differences $a - b$.

1. The first few values are listed in the table below:

p_n	2	3	5	7	11	13	17	19	23	29
k	1	1	1	1	13	17	1	41	157	1811

2. There are 2^n partitions of P_n of the kind we are interested in. You can approach this problem simply by running through all these partitions and find the minimum difference $a - b$. This direct approach isn't as silly as it may sound. Each partition can be encoded as a string of length n of 0s and 1s; a 0 in the i^{th} place meaning that the i^{th} prime is in A. You just need to run through the various possible strings and keep track of the smallest difference. This is a nice little programming exercise.

[1]Christian Aebi is a member of staff at Collège Calvin, Geneva, Switzerland 1211; christian.aebi@edu.ge.ch

[2]Grant Cairns is an Associate Professor in the School of Engineering and Mathematical Sciences, La Trobe University, Melbourne, Australia 3086; G.Cairns@latrobe.edu.au

[3]By convention the product of the elements of the empty set equals 1.

3. In a completely different approach, the information that you are given can be written as equations. Consider the product of the first n primes. This is denoted $p_n\#$ and is known as the n^{th} *primorial*. We have two equations: $a \cdot b = p_n\#$ and $a - b = k$. Substituting for b gives a quadratic equation:

$$a^2 - k \cdot a - p_n\# = 0.$$

   In order for this equation to have an integer solution, its discriminant must be a square, that is, $k^2 + 4p_n\#$ is a square. So, starting with $k = 1$, you can compute $k^2 + 4p_n\#$, and then increment k until you obtain a square. If it turns out that k is prime or 1, increment n and repeat.

4. It's nice to compare these methods (and others?) for speed, and for elegance.

5. You will need a computer! You'll also need some software. If you are fortunate enough to have access to Mathematica or Maple, the necessary coding will only take a few lines. Other programs you might use are: Basic, C++, Pascal, Fortran...

6. The answer is given at the end of this article.

Further Problems

Once you start investigating this question with a computer, you will very likely start examining related questions, observe interesting features, and wonder if they hold for all values of n. (Beware, this kind of investigation is very addictive!). Here are two open problems you might like to examine.

Problem B Consider the following question: for what values of p_n, is there a partition A, B of P_n for which $a - b = 1$? This is possible for $p_n = 2, 3, 5, 7, 17$; find the sets A, B in each of these cases. According to [2], Erdös conjectured that these are the only values with $\min(a - b) = 1$, and that this has been verified by Chris Nash up to $n = 600000$.

Problem C Consider the following question: for what values of p_n, is there a partition A, B of P_n for which $a - b$ is the next prime, p_{n+1}? This is possible for $p_n = 5, 7, 11, 13$; find the sets A, B in each of these cases. At present, we don't know of any other value of n for which this condition holds.

Arguing as in hint (iii) above, you will see that the condition in Problem B is equivalent to the condition that $4p_n\# + 1$ is a square. Similarly, the condition in Problem C says that $4p_n\# + p_{n+1}^2$ is a square. These conditions both have solutions for $p_3 = 5$, as $4p_3\# + 1 = 11^2$ and $4p_3\# + 7^2 = 13^2$. We now show that the two conditions don't have a simultaneous solution for any higher prime.

Proposition 0.1 *There is no prime $p_n > 5$ for which $4p_n\# + 1$ and $4p_n\# + p_{n+1}^2$ are both squares.*

Proof The idea is simply that for large numbers, successive odd squares are too far apart. Suppose that $4p_n\# + 1 = x^2$, and $4p_n\# + p_{n+1}^2$ is square. Then $4p_n\# + p_{n+1}^2$ is at least $(x + 2)^2$. Taking the difference we have $p_{n+1}^2 \geq 4x + 5 > 4x$. Thus

$$4p_n\# + 1 = x^2 < \left(\frac{p_{n+1}^2}{4}\right)^2.$$

By Bertrand's postulate (check it out on Wikipedia), $p_{n+1} < 2p_n, p_{n+1} < 4p_{n-1}, p_{n+1} < 8p_{n-1}$ and $p_{n+1} < 16p_{n-1}$. So

$$4p_n\# + 1 < \left(\frac{p_{n+1}^2}{4}\right)^2 < 64 \cdot p_n \cdot p_{n-1} \cdot p_{n-2} \cdot p_{n-3},$$

which is false for $p_n > 13$. In the cases $p_n = 7, 11, 13$, the number $4p_n\# + 1$ isn't square.

In the above problems we are led to look for squares close to $4p_n\#$. What about squares close to $p_n\#$? The factorisations of the numbers $p\# \pm 1$ have been computed up to the 160^{th} prime; see Bos[1]. One striking feature of these numbers is that, so far, they are all square-free. Deciding whether a given large number is square-free or not is a difficult question; see Pegg [4]. In general, the probability that a given arbitrary number is square-free is only about 2/3 (actually $6/\pi^2$; see Harvester[3]). However, the factors of $p\# \pm 1$ are all greater than p, so perhaps it isn't so surprising that they should often be square-free. This should also be true for numbers close to $p\#$. Some small exceptional examples that are good to keep in mind are: $3\#+2 = 2^3$, $3\#+3 = 3^2$, $5\# - 3 = 3^3$, $5\# - 5 = 5^2$ and $5\# + 6 = 6^2$.

Here are a few things we can prove:

Proposition 0.2 *If $p\# + k$ is a square, then k is not a multiple of q^2 for any prime $q \leq p$.*

Proof Suppose that $p\# + k = a^2$ and $k = q^2 b$, for some prime $q \leq p$ and integers a, b. Then a is divisible by q and hence a^2 is divisible by q^2, and thus $p\#$ is divisible by q^2, which is false.

Proposition 0.3 *For each prime p,*

(a) if $p\# + k$ is a square, then k is not a square,

(b) if $p > 2$ and $p\# + k$ is a square, then $p\# - k$ is not a square.

Proof (a) Suppose that $p\# + b^2 = a^2$. Since $p\#$ is even, a^2 and b^2 have the same parity and hence a and b have the same parity. Thus $a^2 - b^2 = (a-b)(a+b) \equiv 0 \pmod 4$. But this is impossible as $p\# \equiv 2 \pmod 4$.

(b) Suppose once again $p\# + k = a^2$ and also that $p\# - k = b^2$. Adding both equalities we get $2p\# = a^2 + b^2$. Looking at this in $\mathbb{Z}_3$ we have $0 \equiv a^2 + b^2 \pmod 3$. But the only squares in $\mathbb{Z}_3$ are 0 and 1. So a and b must both be divisible by 3. But that is in contradiction with $2p\# = a^2 + b^2$, looked at in $\mathbb{Z}_9$.

Although $2\# + 2 = 2^2$, the number $p\# + 2$ is never square for $p > 2$. Indeed, we have:

Proposition 0.4 *Suppose that $p > 2$. If $p\# + k$ is a square, then $k \not\equiv 2 \pmod 3, k \not\equiv 0 \pmod 4$ and $k \not\equiv 1 \pmod 4$. In particular, there is no prime p for which $p\# \pm 1$ is a square.*

Proof We again use the fact that the only squares in $\mathbb{Z}_3$ are 0 and 1. So if $p\# + k = a^2$ and a is not a multiple of 3 then $k \equiv a^2 \equiv 1 \pmod 3$, meaning $k \not\equiv 2 \pmod 3$.

By Proposition 0.2, k isn't a multiple of 4. If k is odd, then a is odd, say $a = 1 + 2i$. Then

$$p\# = -k + a^2 = -k + (1 + 2i)^2 = -k + 1 + 4i + 4i^2.$$

In modulo 4 this gives $2 \equiv -k + 1$, that is, $k \equiv 3$. So $k \not\equiv 1 \pmod 4$. This completes the proof.

Indeed, we have $3\# - 2 = 2^2$. Question: is there a $p > 3$ for which $p\# - 2$ is a square?

Indeed, we have $3\# + 3 = 3^2$. Question: is there a $p > 3$ for which $p\# + 3$ is a square?

The answer to both these questions is no. Indeed, we have

Proposition 0.5 *Suppose that $p > 3$. If $p\# + k$ is a square, then modulo $2^2 \cdot 3^2 \cdot 5 = 180$, k is congruent to one of the following:*

$$6, 10, 15, 19, 30, 31, 34, 39, 46, 51, 55, 66, 70, 79, 91, 94,$$
$$106, 111, 114, 115, 130, 139, 151, 154, 159, 166, 174.$$

Proof First note that by Proposition 0.2, k isn't a multiple of 9 or 25. Secondly, note that modulo 5, $p\# + k = a^2$ gives $k \equiv 0$ or ± 1. These observations, together with the previous proposition, give the required result.

We have $5\# + 6 = 6^2$. Question: is there a $p > 5$ for which $p\# + 6$ is a square? The answer is no. Indeed, we have

Proposition 0.6 *Suppose that $p > 5$. If $p\# + k$ is a square, then modulo $2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$, k is congruent to one of the following:*

$$15, 30, 39, 46, 51, 70, 79, 91, 106, 114, 130, 151, 154, 186, 190, 210, 211, 214, 219, 226, 231,$$
$$235, 246, 259, 274, 291, 295, 310, 319, 330, 331, 354, 366, 379, 394, 399, 406, 415, 435, 466,$$
$$471, 499, 511, 519, 526, 534, 546, 555, 571, 574, 595, 606, 610, 631, 634, 646, 651, 655, 679,$$
$$690, 694, 714, 715, 730, 735, 739, 751, 771, 786, 795, 799, 814, 826, 834, 835, 870, 879, 886,$$
$$910, 919, 939, 946, 966, 970, 991, 994, 1015, 1030, 1051, 1054, 1059, 1066, 1086, 1099, 1110,$$
$$1114, 1131, 1135, 1155, 1159, 1171, 1191, 1194, 1219, 1234, 1239, 1246, 1254, 1255.$$

Proof In modulo 7, $p\# + k = a^2$ gives $k \equiv 0, 1, 2$ or 4. This, together with the previous propositions, give the required result.

We have $7\# + 15 = 15^2$. Question: is there a $p > 7$ for which $p\# + 15$ is a square? Not surprisingly, the answer is again no. But this time we don't get it by just going to the next prime, 11, because $15 \equiv 2^2 \pmod{11}$. However, we can verify directly that $11\# + 15 = 2325$ is not a square, and then use the fact that 2 is not a quadratic residue modulo 13. Of course, we can continue in this manner. From a computational perspective, if one is searching for the smallest k such that $p\# + k$ is square, it is much quicker to compute $\sqrt{p_n\#}$ and square its ceiling (i.e., the least integer greater than $\sqrt{p_n\#}$); subtracting $p\#$ gives k. In this way one can very quickly compute k for p_n up to $n = 1000$. The table below gives some values. From the table it may appear that k is growing monotonically with p.

Problem D Does k grow monotonically with p? If not, find the smallest p_n such that the k for p_{n+1} is smaller than the k for p_n.

Another observation we might make from the table is that there seem to be very few prime values of k.

Problem E Find the smallest $p_n > 3$ for which k is prime.

p	$p\#$	the smallest k such that $p\# + k$ is square	$\sqrt{p\# + k}$
2	2	2	2
3	6	3	3
5	30	6	6
7	210	15	15
11	2310	91	49
13	30030	246	174
17	510510	715	715
19	9699690	3535	3115
23	223092870	21099	14937
29	6469693230	95995	80435
31	200560490130	175470	447840
37	7420738134810	4468006	2724104
41	304250263527210	31516774	17442772
43	13082761331670030	192339970	114379900
47	614889782588491410	212951314	784149082
53	32589158477190044730	5138843466	5708691486

Another striking feature of this table is that for $p = 2, 3, 5, 7$ and 17, the smallest k for which $p\# + k$ is square satisfies $p\# + k = k^2$. Are there any more such primes? Notice that the condition that the quadratic equation $p\# + k = k^2$ has an integer solution for k, is equivalent to the condition that $1 + 4 \cdot p\#$ is a square; so we arrive at the same condition as for problem B. Moreover, notice that if $p\# + k = k^2$, then subtracting $2k - 1$ gives $p\# - (k-1) = k^2 - 2k + 1 = (k-1)^2$. We make two observations:

1. The square $(k-1)^2$ is closer to $p\#$ than the square k^2.

2. Since $(k-1)^2, k^2$ are consecutive squares and one is less than $p\#$ and the other is greater than $p\#$, there is no other square closer to $p\#$.

Thus when the condition in problem B has a solution, $p_n\#$ lies as close as possible to the middle of consecutive squares. Let us record this more precisely as a proposition:

Proposition 0.7 *Let l^2 denote the least square greater than $p_n\#$, and let g^2 denote the greatest square less than $p_n\#$. Then there is a partition A, B of P_n for which* $\min |a - b| = 1$ *if and only if the average $\frac{l^2+g^2}{2}$ is $p_n\# + \frac{1}{2}$.*

Proof We have already established one direction. So suppose that

$$\frac{l^2 + g^2}{2} = p_n\# + \frac{1}{2}. \tag{0.1}$$

Let $l^2 = p_n\# + k$. From (0.1) we have $g^2 = p_n\# - k + 1$. As $l = g + 1$ we get

$$p_n\# + k = l^2 = g^2 + 2g + 1 = p_n\# - k + 1 + 2g + 1,$$

and hence $g = k - 1$ and $l = k$. Thus $p_n\# + k = k^2$, and so $1 + 4 \cdot p\#$ is a square; this gives us the required conclusion.

Problem F We saw in Proposition 0.3(b) that $p_n\#$ can never be the average of two squares. Explain why there cannot exist two squares whose average is $p_n\# - \frac{1}{2}$.

Solutions to Problems

Problem A

For $n = 13$, the smallest difference is $k = 95533 = 83 \cdot 1151$.

Problem B

$2 - 1 = 1, \quad 3 - 2 = 1, \quad 3 \cdot 2 - 5 = 1, \quad 3 \cdot 5 - 2 \cdot 7 = 1.$

Problem C

$2 \cdot 5 - 3 = 7, \quad 3 \cdot 7 - 2 \cdot 5 = 11, \quad 5 \cdot 11 - 2 \cdot 3 \cdot 7 = 13.$

Problem D

For $p_n = 197$, we have $k = 759193255702310714280104837320500174661 9$.

$$2 \cdot 7 \cdot 13 - 3 \cdot 5 \cdot 11 = 17.$$

Problem E

For $p_n = 11779$, the number $k = 630 \ldots 811$ is prime; it has 2516 digits while for $p_{n+1} = 199$, we have

$$k = 861993745812359750296203700298062752346.$$

Problem F

In modulo 4, we have $2p_n\# - 1 \equiv 3$, while $x^2 + y^2 = 0, 1$ or 2.

References

[1] Joppe Bos, *The factorization of primorials* ± 1 (web page), http://primorial.unit82.com/ (Editorial note, January 2014: this is now a dead link, but see also http://donovanjohnson.com/primorial3.html)

[2] John Harvester, *The prime puzzle & problems connection* (web page), http://www.primepuzzles.net/conjectures/conj_018.htm

[3] Karl Greger, *Square divisors and square-free numbers*, Math. Mag., **51** (1978), no. 4, 211–219.

[4] Ed Pegg Jr., *The Möbius Function (and squarefree numbers)* (web page), http://www.mathpuzzle.com/MAA/02-Mobius Function/mathgames_11_03_03.html