On the Products of Twin Primes

Michael G. Kaarhus

February 19, 2013

Abstract

This article answers elementary questions about the products of twin primes.

I am obliged to begin with this caveat: I have not read on the subject of multiplying twin primes. And so, I don't know if anyone else has written on this. I simply wish to write about it, even though I haven't read about it.

This is a very simple topic, mathematically speaking. Yet, amateurs such as myself wonder about simple things, such as these:

- Why is the product of a pair of twin primes always $\equiv 5 \pmod 6$?
- Given any two twin prime pairs (p, r), and (p_2, r_2), why is $p \cdot r_2$ always $\equiv 5 \pmod 6$?
- Why is $p \cdot p_2$ always $\equiv 1 \pmod 6$?
- Why is $r \cdot r_2$ always $\equiv 1 \pmod 6$?

Here I explicate the above. To understand my explications, you must first understand modulo arithmetic. Click here for a primer on modulo arithmetic. From that primer, you will understand (among other things) that, for all prime pairs $\geq (5, 7)$:

- The central composite q of the prime pair (p, r) is $\equiv 0 \pmod 6$
- All p are $\equiv 5 \pmod 6$. For example, $11 \equiv 5 \pmod 6$
- All r are $\equiv 1 \pmod 6$. For example, $13 \equiv 1 \pmod 6$

The principles explicated here can actually be applied to any two integers having a difference of 2, where the central integer will not necessarily be $\equiv 0 \pmod 6$. But prime pairs provide a convenient example, so I will begin with prime pairs.

Theorem 1. $p \cdot r \equiv 5 \pmod 6$

Proof. Begin with the fact that (all central composites q) $\equiv 0 \pmod 6$. If you add or subtract any number of q's to or from q, you will get another integer that is also $\equiv 0 \pmod 6$. You can say that like this:

$$q \cdot n \equiv 0 \pmod 6, \text{ where n is an integer.}$$

We can even let $n = q$, in which case we have

$$q^2 \equiv 0 \pmod 6.$$

Now see that $(p, r) = (q-1, q+1)$, and multiply:

$$(q-1) \cdot (q+1) = q^2 - 1.$$

I just showed that $q^2 \equiv 0 \pmod 6$, so it must be that

$$q^2 - 1 \equiv 5 \pmod 6. \text{ And that's it! That's why } p \cdot r \equiv 5 \pmod 6.$$

In case you still don't see, maybe you forgot that

$$\begin{aligned} p \cdot r &= (q-1) \cdot (q+1) \\ &= q^2 - 1. \quad \text{And } q^2 - 1 \equiv 5 \pmod 6, \ \big(\text{because } q^2 \equiv 0 \pmod 6\big). \end{aligned}$$

□

Now let's broaden to a more general case:

Theorem 2. *$(p \cdot r_2) \equiv 5 \pmod 6$, where r_2 is* any r

Proof. We can represent the above this way:

$$p \cdot r_2 = (q-1) \cdot (6n+1), \text{ where } n \text{ is a positive integer.}$$

Granted, $(6n+1)$ will not be the second twin of a prime pair for all n. However, if you keep trying larger and larger n, you will eventually get a $(6n+1)$ that is the second twin of a prime pair. Expand the binomial:

$$(q-1) \cdot (6n+1) = 6nq + q - 6n - 1. \text{ Consider each term.}$$

$6nq$ is just some multiple of 6. So we can be sure that
$6nq \equiv 0 \pmod 6$.
$q - 6n$ is just some multiple of 6. So, we can be sure that
$q - 6n \equiv 0 \pmod 6$. And we can generalize:

$$(q-1) \cdot (6n+1) = (\text{some multiple of } 6) - (\text{some multiple of } 6) - 1.$$

In other words,
$p \cdot r_2 = (\text{some integer}) \equiv 0 \pmod 6 - 1$.
$p \cdot r_2 = (\text{some integer}) \equiv 5 \pmod 6$. □

Theorem 3. $p^2 \equiv 1 \pmod 6$.

Proof. This is the simplest case:

$$\begin{aligned} p^2 &= (q-1)\cdot(q-1) \\ &= q^2 - 2q + 1 \end{aligned}$$

$q^2 - 2q$ is just some multiple of q, and q is just some multiple of 6. So

$$q^2 - 2q \equiv 0 \pmod 6, \text{ and}$$

$$q^2 - 2q + 1 \equiv 1 \pmod 6.$$

□

Now we get fancier: $p_2 > p$

Theorem 4. $(p \cdot p_2) \equiv 1 \pmod 6$.

Proof. $p \cdot p_2 = (q-1)\cdot(6n-1)$ for some positive integer n.

$$(q-1)\cdot(6n-1) = 6nq - q - 6n + 1. \text{ Consider the terms.}$$

$6nq$ is just some multiple of 6. Therefore,

$$6nq \equiv 0 \pmod 6.$$

$-q - 6n$ is just some negative multiple of 6. Therefore,

$$-q - 6n \equiv 0 \pmod 6. \text{ To generalize,}$$

$$(q-1)\cdot(6n-1) = (\text{some multiple of } 6) - (\text{some multiple of } 6) + 1. \text{ Or}$$

$$(q-1)\cdot(6n-1) = (\text{some integer}) \equiv 0 \pmod 6 + 1, \text{ which means}$$

$$(q-1)\cdot(6n-1) = (\text{some integer}) \equiv 1 \pmod 6 \text{ Or,}$$

$$p \cdot p_2 = (\text{some integer}) \equiv 1 \pmod 6$$

□

Theorem 5. $(r \cdot r_2) \equiv 1 \pmod 6$. *where* r_2 *is any* r

Proof. In the simplest case, $r_2 = r$, and

$$\begin{aligned} r^2 &= (q+1)\cdot(q+1) \\ &= q^2 + 2q + 1 \end{aligned}$$

$q^2 + 2q$ is just some multiple of q, and q is just some multiple of 6. So

$$q^2 + 2q \equiv 0 \pmod 6, \text{ and}$$

$$q^2 + 2q + 1 \equiv 1 \pmod 6.$$

Now we get fancier: $r_2 > r$

$$r \cdot r_2 = (q+1)\cdot(6n+1) \text{ for some positive integer n.}$$

$$(q+1)\cdot(6n+1) = 6nq + q + 6n + 1. \text{ Consider the terms.}$$

$6nq$ is just some multiple of 6. Therefore,

$$6nq \equiv 0 \pmod 6.$$

$q + 6n$ is just some multiple of 6. Therefore,

$$q + 6n \equiv 0 \pmod 6. \text{ To generalize,}$$

$$(q+1)\cdot(6n+1) = (\text{some multiple of } 6) + (\text{some multiple of } 6) + 1. \text{ Or}$$

$$(q+1)\cdot(6n+1) = (\text{some integer}) \equiv 0 \pmod 6 + 1, \text{ which means}$$

$$(q+1)\cdot(6n+1) = (\text{some integer}) \equiv 1 \pmod 6 \text{ Or,}$$

$$r \cdot r_2 = (\text{some integer}) \equiv 1 \pmod 6$$

□

Finally, consider a not-so-intuitive formula: For any two positive integers that differ by only 2 (this includes any prime pair (p, r)),

$$p + r = \frac{r^2 - p^2}{2}$$

How do I get that? Elementary!

$$\begin{aligned} q^2 - 1 &= (p+1)^2 - 1 \\ &= p^2 + 2p \\ q^2 - 1 &= (r-1)^2 - 1 \\ &= r^2 - 2r \\ p^2 + 2p &= r^2 - 2r \\ 2p + 2r &= r^2 - p^2 \\ p + r &= \frac{r^2 - p^2}{2} \end{aligned}$$

To make the above true for both positive and negative integers,

$$|p+r| = \frac{r^2 - p^2}{2}$$

Specifically for the prime pair (p, r),

$$\begin{aligned} p + r &= (q-1) + (q+1) = 2q. \text{ Therefore,} \\ p + r &\equiv 0 \pmod 6. \text{ Therefore,} \\ \frac{r^2 - p^2}{2} &\equiv 0 \pmod 6 \end{aligned}$$

Copyright