Primes and their distribution

DEFINITION: LET $a \in \mathbb{Z}$, $a \notin \{-1, 0, 1\}$. WE SAY THAT a IS PRIME IF ITS ONLY DIVISORS ARE ± 1 AND $\pm P$. IF a IS NOT PRIME THEN WE SAY THAT a IS COMPOSITE.

EXERCISE: LET $a \in \mathbb{Z}$, $a \notin \{-1, 0, 1\}$. SHOW THERE EXISTS A POSITIVE PRIME P SUCH THAT $P | a$. IN PARTICULAR, IF $a \in \mathbb{N}$ IS NOT A PRIME, THERE EXISTS A POSITIVE PRIME $P < a$ SUCH THAT $P | a$.

SOLUTION: LET $a \in \mathbb{Z}$, $a \notin \{-1, 0, 1\}$. LET S BE THE SET

$$S = \{ m \in \mathbb{N} : m \geq 2 \text{ and } m | a \}.$$

NOTE THAT $S \subseteq \mathbb{N}$. MOREOVER, IF $a > 0$ THEN $a \geq 2$ AND $a | a$ WHICH IMPLIES THAT $a \in S$. SIMILARLY, IF $a < 0$ THEN $a \leq -2$ AND SO $-a \in S$ SINCE $-a \geq 2$ AND $-a | a$. THIS SHOWS THAT S IS NOT EMPTY. HENCE, BY THE WELL-ORDERING PRINCIPLE, S CONTAINS A LEAST ELEMENT. LET P DENOTE SUCH A NUMBER. THEN, $P \in \mathbb{N}$, $P \geq 2$, $P | a$ AND $P \leq m$ FOR ALL $m \in S$. LET'S PROVE THAT P IS PRIME. IT SUFFICES TO SHOW THAT THE ONLY POSITIVE DIVISORS OF P ARE $1, P$. NOTE THAT $1 | P$. LET $d \in \mathbb{N}$ SUCH THAT $d | P$ AND $d \neq 1$. SINCE $d \in \mathbb{N}$, $d \neq 1$ WE HAVE $d \geq 2$. IN ADDITION, AS $d | P$ AND $P | a$ WE HAVE $d | a$. THEN, $d \in S$ AND $P \leq d$ AS P IS THE LEAST ELEMENT OF S. ON THE OTHER HAND, SINCE $d, P \in \mathbb{N}$ AND $d | P$ WE HAVE $d \leq P$. THIS SHOWS

THAT $d=p$. THEN, $\mathrm{Div}^+(p) = \{1, p\}$. WE THEREFORE HAVE THAT p IS PRIME, $p \in \mathbb{N}$ AND p/a.

SUPPOSE NOW THAT $a \in \mathbb{N}$ IS NOT A PRIME. THEN, FROM THE ABOVE COMMENTS, THERE EXISTS $p \in \mathbb{N}$ SUCH THAT p IS PRIME AND p/a. SO, $p \leq a$. SINCE p IS PRIME AND a IS NOT PRIME, THE CASE $a=p$ CANNOT HAPPEN. SO, IF $a \in \mathbb{N}$ IS NOT A PRIME, THERE EXISTS A POSITIVE PRIME $p < a$ SUCH THAT p/a.

EXERCISE: LET $a \in \mathbb{N}$, $a \neq 1$. IF a IS NOT PRIME THEN THERE EXISTS A PRIME p SUCH THAT $1 < p \leq \sqrt{a}$ AND p/a.

SOLUTION: LET $a \in \mathbb{N}$, $a \neq 1$. SUPPOSE a IS NOT PRIME. LET S BE THE SET $S := \{ m \in \mathbb{N} : m \text{ is prime and } m/a \}$. NOTE THAT $S \subseteq \mathbb{N}$ AND $S \neq \emptyset$ BY THE PREVIOUS EXERCISE. SO, BY THE WELL-ORDERING PRINCIPLE, S HAS A LEAST ELEMENT. LET p DENOTE SUCH A NUMBER. THEN, $p \in \mathbb{N}$, p IS PRIME, p/a, $p < a$ AND $p \leq m$ FOR EVERY $m \in S$. SINCE p/a, THERE EXISTS $b \in \mathbb{Z}$ SUCH THAT $a = p \cdot b$. NOTE THAT $b \in \mathbb{N}$ SINCE $a \in \mathbb{N}$, $p \in \mathbb{N}$. WE ALSO OBSERVE THAT $b \neq 1$. OTHERWISE, IF $b=1$, WE HAVE $a=p$ CONTRADICTING THAT $p < a$. THEN, SINCE $b \in \mathbb{N}$, $b \neq 1$, THERE EXISTS A POSITIVE PRIME q SUCH THAT q/b. SINCE q/b AND b/a WE HAVE q/a. THIS SHOWS THAT $q \in S$ AND SO $p \leq q$. WE ALSO OBSERVE $q \leq b$

SINCE $q|b$ AND $q, b \in \mathbb{N}$. WE THUS HAVE

$$p^2 = p.p \leq p.q \leq p.b = a.$$

HENCE, IF $a \in \mathbb{N}$, $a \neq 1$ IS NOT PRIME, THERE EXISTS A PRIME p SUCH THAT $p|a$ AND $1 < p \leq \sqrt{a}$.

EXERCISE: FIND ALL POSITIVE PRIME NUMBERS LESS OR EQUAL THAN 38. IS 1009 A PRIME NUMBER?

SOLUTION: LET'S WRITE THE FIRST 38 NATURAL NUMBERS:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38		

BY A PREVIOUS EXERCISE, RECALL IF $a \in \mathbb{N}$, $a \neq 1$ IS NOT A PRIME NUMBER, THERE EXISTS $p \in \mathbb{N}$ PRIME SUCH THAT $p < a$ AND $p|a$. $(*)$

BY DEFINITION, 1 IS NOT A PRIME. SO WE DELETE 1 FROM OUR LIST. SUPPOSE NOW THAT 2 IS NOT A PRIME. THEN, BY $(*)$ THERE IS A PRIME p SUCH THAT $1 < p < 2$ AND $p|2$ WHICH IS NOT POSSIBLE. SO, 2 IS PRIME. IN ADDITION, EVERY MULTIPLE OF 2 LESS OR EQUAL THAN 38 IS NOT A PRIME NUMBER. SO, WE CAN DELETE THEM FROM OUR LIST:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38		

NOW, THE FIRST OF THE REMAINING INTEGER IS 3 WHICH MUST BE A PRIME. OTHERWISE, IF 3 IS NOT A PRIME, THERE EXIST $p \in \mathbb{N}$ SUCH THAT $1 < p < 3$ AND $p \mid 3$. THEN $p = 2$ BUT $2 \nmid 3$, A CONTRADICTION. SIMILARLY, ALL THOSE NUMBERS DIVISIBLE BY 3 LESS THAN 38 IS NOT IN THE LIST:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38		

THE SMALLEST INTEGER AFTER 3 THAT HAS NOT YET BEEN DELETED IS 5. BUT BY (*), 5 IS PRIME SINCE 5 IS NOT DIVISIBLE BY EITHER 2 OR 3. IN ADDITION, ALL PROPER MULTIPLES OF 5 ARE REMOVED SINCE THEY ARE COMPOSITE.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38		

THE NEXT SURVIVING INTEGER IN THE LIST IS 7 WHICH IS NOT DIVISIBLE BY 2, 3, 5, THE ONLY PRIME THAT PRECEDE IT. SO, 7 IS PRIME. NOTE NOW ALL THE PROPER MULTIPLES OF 7 WERE ELIMINATED. REPEATING THESE STEPS, IT

IS EASY TO SEE THE SURVIVING INTEGERS IN THE LIST :

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38		

THEREFORE, IF P IS PRIME AND $1 < P \leq 38$ THEN

$$P \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}.$$

WE NEXT DETERMINE IF 1009 IS A PRIME NUMBER. SUPPOSE THAT 1009 IS NOT A PRIME. THEN, AS $1009 \in \mathbb{N}$, $1009 \neq 1$, THERE EXISTS A PRIME P SUCH THAT $1 < P < \sqrt{1009} < 32$ AND $P \mid 1009$.

THEN, BY THE ABOVE COMMENTS,

$$P \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}.$$

BY THE ALGORITHM DIVISION THEOREM, WE OBSERVE:

$1009 = 2 \cdot 504 + 1$	$1009 = 11 \cdot 91 + 8$	$1009 = 23 \cdot 43 + 20$
$1009 = 3 \cdot 336 + 1$	$1009 = 13 \cdot 77 + 8$	$1009 = 29 \cdot 34 + 23$
$1009 = 5 \cdot 201 + 4$	$1009 = 17 \cdot 59 + 6$	$1009 = 31 \cdot 32 + 17$
$1009 = 7 \cdot 144 + 1$	$1009 = 19 \cdot 53 + 2$	

THIS SHOWS THAT $P \nmid 1009$ WHICH IS A CONTRADICTION. WE THUS HAVE 1009 IS PRIME.

EXERCISE: LET $a \in \mathbb{Z}$ AND LET $P \in \mathbb{N}$ BE A PRIME NUMBER. FIND $\gcd(a, P)$.

SOLUTION: LET $a \in \mathbb{Z}$ AND LET $p \in \mathbb{N}$ A PRIME. SUPPOSE FIRST THAT $p|a$. THEN, SINCE $p|p$, WE HAVE p IS A COMMON DIVISOR OF a AND p. IF THERE EXISTS $c \in \mathbb{Z}$ SUCH THAT $c|a$ AND $c|p$ THEN $c \leq |c| \leq p$ AND SO, $c \leq p$. THIS SHOWS THAT $\gcd(a,p) = p$ IF $p|a$. SUPPOSE NEXT THAT $p \nmid a$. LET $d = \gcd(a,p)$. NOTE THAT $d|a$ AND $d|p$. SINCE $d|p$ THEN, AS p IS PRIME, $d \in \{1,p\}$. BUT $d \neq p$ AS $p \nmid a$. THEREFORE, $d = 1$ IF $p \nmid a$. WE THUS HAVE

$$\gcd(a,p) = \begin{cases} p & \text{if } p|a \\ 1 & \text{if } p \nmid a \end{cases}$$

PREPOSITION: IF p IS A PRIME AND $p|ab$ THEN $p|a$ OR $p|b$.

COROLLARY: IF p IS A PRIME AND $p|a_1.a_2.\ldots.a_m$ THEN $p|a_j$ FOR SOME j, WHERE $1 \leq j \leq m$.

EXERCISE: LET p BE A PRIME. IF p HAS REMAINDER 1 IN THE DIVISION BY 3, FIND THE REMAINDER IN THE DIVISION OF p BY 6.

SOLUTION: LET p BE A PRIME. SINCE p HAS REMAINDER 1 IN THE DIVISION BY 3, BY THE ALGORITHM DIVISION THEOREM, THERE EXISTS $q \in \mathbb{Z}$ SUCH THAT $p = 3q+1$. NOTE THAT $p \neq 2$. IN FACT, IF $p=2$, THEN $2 = 3q+1$ IMPLIES THAT $3q = 1$ AND SO $3|1$ WHICH IS A

CONTRADICTION. IF $P=-2$ THEN $P=-2=3.(-1)+1$ AND SO $P=3.\left(2(-1)+1\right)+1=6.(-1)+4$. THEN, BY THE ALGORITHM DIVISION THEOREM, SINCE THE QUOTIENT AND THE REMAINDER IN THE DIVISION BY 6 ARE UNIQUE, WE HAVE THE REMAINDER IN THE DIVISION BY 6 EQUALS 4 IF $P=-2$. SUPPOSE NEXT THAT $P\neq -2$. THEN, P IS ODD AND SO $P-1=3q$ IS EVEN. THIS SHOWS THAT $2|3q$ AND SINCE $(2,3)=1$ WE HAVE $2|q$. SO, THERE EXISTS $k\in\mathbb{Z}$ SUCH THAT $q=2k$. THEN,

$$P=3q+1=3.(2k)+1=6k+1.$$

THEREFORE, BY THE ALGORITHM DIVISION THEOREM, SINCE THE QUOTIENT AND THE REMAINDER IN THE DIVISION BY 6 ARE UNIQUE, WE HAVE THE REMAINDER IN THE DIVISION BY 6 EQUALS 1 IF $P\neq -2$. THE RESULT FOLLOWS.

EXERCISE: SHOW THE ONLY POSITIVE PRIME OF THE FORM m^3-1 IS 7.

SOLUTION: LET $P>1$ BE A PRIME SUCH THAT $P=m^3-1$ FOR SOME $m\in\mathbb{N}$. AS $P>1$ WE OBSERVE $m\geq 2$. NOTE THAT $m-1 \mid m^3-1$ AND SO $m-1 \mid P$. SINCE P IS PRIME, EITHER $m-1=1$ OR $m-1=P$. SUPPOSE $m=P+1$. THEN $P=(P+1)^3-1$ WHICH IMPLIES $(P+1)=(P+1)^3$. SO, $P+1$ IS A SOLUTION OF THE EQUATION $x=x^3$ AND SO $P+1\in\{-1,0,1\}$. HENCE, $P\in\{-2,-1,0\}$ WHICH is a contradiction since $p > 1$. We therefore have $m = 2$ and $p = m^3 - 1 = 2^3 - 1 = 7$.

EXERCISE: The only positive prime p for which $3p+1$ is a perfect square is $p = 5$.

SOLUTION: Let $p > 1$ be a prime number such that $3p+1 = m^2$ for some $m \in \mathbb{N}$. Then $3p = m^2 - 1 = (m-1)(m+1)$ and so $m+1 \mid 3p$. Since p is prime then we have $m+1 \in \{\pm 1, \pm 3, \pm p, \pm 3p\}$. But $m+1 > 0$ implies $m+1 \in \{1, 3, p, 3p\}$. As $p > 1$, $m^2 = 3p+1 > 4$ and so $m > 2$. Then $m+1 > 3$. If $m+1 = p$ then $3p = (m-1)(m+1) = (p-2)p$ implies $[(p-2)-3]p = 0$ and so $p = 5$ as $p > 1$. If $m+1 = 3p$ we have $3p = (3p-2)3p$ and so $p = 1$ contradicting $p > 1$. We therefore have $p = 5$ is the only prime which such property.

EXERCISE: Prove the only positive prime of the form $m^2 - 4$ is 5.

SOLUTION: Let $p > 1$ be a prime such that $p = m^2 - 4$ for some $m \in \mathbb{N}$. Then, $p = m^2 - 4 = (m-2)(m+2)$ and so $m+2 \mid p$. This means that $m+2 \in \{\pm 1, \pm p\}$. Since $m+2 > 0$ we have $m+2 \in \{1, p\}$. Since $m \in \mathbb{N}$, observe $m+2 \neq 1$. We therefore have $m+2 = p$. Hence, $p = (p-4)p$ and since $p > 1$, $(p-5)p = 0$ we get $p = 5$.

EXERCISE: if $p \geq 5$ is a prime number, show that p^2+2 is composite.

SOLUTION: Let $p \geq 5$ be a prime number. By the Division Algorithm Theorem, there exist unique integers q, r such that $p = 6.q + r$ where $r \in \{0,1,2,3,4,5\}$. Note that $r \in \{1,5\}$ as $p \geq 5$ is prime. In fact, the only positive divisors of p are 1 and p. So, if $r \in \{0,2,4\}$ then $2 | r$ and since $2 | 2.3q = 6q$ we have $2 | 6q+r = p$ contradicting that p is prime. Similarly, if $r=3$ then $p = 6q+3 = 3(2q+1)$ and so, $3 | p$ which is a contradiction. Then either $p = 6q+1$ or $p = 6q+5$.

We now notice $p^2+2 = (6q+r)^2+2 = 36q^2 + 12qr + r^2 + 2$. So, if $r=1$ then $r^2+2 = 3$ while $r^2+2 = 27$ if $r=5$. We therefore have $3 | r^2+2$. As $3 | 36q^2+12qr$ we thus have $3 | (36q^2+12qr)+(r^2+2)$, that is $3 | p^2+2$. This shows that p^2+2 is composite.

EXERCISE: Given that p is a prime and $p | a^m$ for some $m \in \mathbb{N}$, prove that $p^m | a^m$. In addition, if $\gcd(a,b) = p$, find all the possible values of $\gcd(a^3, b^2)$.

SOLUTION: Since p is a prime an $p | a^m$ then we have that $p | a$. Then, there exists $k \in \mathbb{Z}$ such that $a = p.k$. Hence, $a^m = (pk)^m = p^m.k^m$ with $k^m \in \mathbb{Z}$ which shows than $p^m | a^m$.

Suppose now that $\gcd(a,b) = p$. Then, there exist $s,t \in \mathbb{Z}$ such that $a = ps$, $b = pt$ and $(s,t) = 1$. Since $(s^3,t^2) = 1$, we also notice that

$$\gcd(a^3,b^2) = \gcd(p^3.s^3, p^2.t^2) = p^2.\gcd(ps^3, t^2) = p^2.\gcd(p, t^2).$$

Recall that if $(a,b) = 1$ then $(ac,b) = (c,b)$ for every $c \in \mathbb{Z}$.

WE NEXT CLAIM THAT $\gcd(p, t^2) = \begin{cases} |p| & \text{if } p \mid t \\ 1 & \text{if } p \nmid t \end{cases}$.

TO PROVE OUR CLAIM, SUPPOSE FIRST THAT $p \mid t$. THEN, $p \mid t^2$ AND $p \mid p$ WHICH IMPLIES THAT $|p| \mid t^2$ AND $|p| \mid p$. THEN, $|p|$ IS A COMMON DIVISOR OF p AND t^2. NOW, IF $c \in \mathbb{Z}$ IS A COMMON DIVISOR OF p AND t^2 THEN $c \mid p$ AND SO $c \leq |c| \leq |p|$. THIS SHOWS $\gcd(p, t^2) = |p|$ IF $p \mid t$. ON THE OTHER HAND, IF $p \nmid t$ THEN $\gcd(p, t) = 1$. WE THUS HAVE $\gcd(p, t^2) = \gcd(t^2, p) = \gcd(t, p) = \gcd(p, t) = 1$. THIS PROVES OUR CLAIM. THEREFORE,

$$\gcd(a^3, b^2) = p^2 \cdot \gcd(p, t^2) = \begin{cases} |p|^3 & \text{if } p \mid t \\ p^2 & \text{if } p \nmid t \end{cases}.$$

EXERCISE: LET $m \in \mathbb{N}$, $m > 1$. PROVE THAT $m^4 + 4$ IS COMPOSITE.

SOLUTION: LET $\mathbb{C}[x]$ THE SET OF ALL POLYNOMIALS IN THE INDETERMINATE x WHERE THE COEFFICIENTS ARE COMPLEX NUMBERS. LET $p \in \mathbb{C}[x]$ GIVEN BY $p(x) = x^4 + 4$. WE OBSERVE $z \in \mathbb{C}$ IS A ROOT OF p IFF $p(z) = z^4 + 4 = 0$. THIS MEANS THAT ALL ROOTS OF p ARE THE 4-TH ROOTS OF -4. THAT IS, z IS A ROOT OF p IFF $z = w_k = \sqrt[4]{4} \cdot \left[\cos\left(\frac{2k+1}{4}\pi\right) + i \sin\left(\frac{2k+1}{4}\pi\right)\right]$ FOR $k \in \{0, 1, 2, 3\}$. SO, IT IS EASY TO SEE THAT $w_0 = 1 + i$, $w_1 = -1 + i$, $w_2 = -1 - i$, $w_3 = 1 - i$. WE ALSO NOTE THAT $w_3 = \overline{w_0}$ AND $w_2 = \overline{w_1}$. CONSEQUENTLY, WE CAN WRITE

$$\begin{aligned} p(x) &= (x - w_0)(x - w_1)(x - w_2)(x - w_3) = (x - w_0)(x - w_3)(x - w_1)(x - w_2) \\ &= (x - w_0)(x - \overline{w_0})(x - w_1)(x - \overline{w_1}) = \left(x^2 - (w_0 + \overline{w_0})x - w_0\overline{w_0}\right)\left(x^2 - (w_1 + \overline{w_1})x - w_1\overline{w_1}\right) \\ &= \left(x^2 - 2\operatorname{Re}(w_0)x - |w_0|^2\right) \cdot \left(x^2 - 2\operatorname{Re}(w_1)x - |w_1|^2\right) \\ &= (x^2 - 2x - 2) \cdot (x^2 + 2x - 2) \end{aligned}$$

RECALL THAT $z + \overline{z} = 2\operatorname{Re}(z)$, $z \cdot \overline{z} = |z|^2$ AND $\operatorname{Re}(z)^2 + \operatorname{Im}(z)^2 = |z|^2$ FOR EVERY $z \in \mathbb{C}$.

HENCE, EVERY INTEGER OF THE FORM $m^4 + 4$, WITH $m \in \mathbb{N}$, $m > 1$ CAN BE WRITTEN AS FOLLOWS: $m^4 + 4 = (m^2 - 2m - 2) \cdot (m^2 + 2m - 2)$. WE OBSERVE $m^2 + 2m - 2 > 1$

SINCE $m>1$ AND $m^2+2m-2 \mid m^4+4$. THIS MEANS THAT m^4+4 IS COMPOSITE.

EXERCISE: LET $m \in \mathbb{N}$. IF $m>4$ IS COMPOSITE THEN m DIVIDES $(m-1)!$.

SOLUTION: LET $m>4$ BE A COMPOSITE NUMBER. THEN THERE EXIST $s,t \in \mathbb{Z}$, $1 < s,t < m$ SUCH THAT $s.t = m$. SUPPOSE THAT $s \neq t$. THEN $s \leq m-1$ AND $t \leq m-1$ IMPLIES THAT s AND t ARE BOTH FACTORS OF $(m-1)!$. SO,

$$(m-1)! = s.t. \prod_{\substack{1\leq k\leq m-1 \\ k\neq s,\, k\neq t}} k = m. \prod_{\substack{1\leq k\leq m-1 \\ k\neq s,\, k\neq t}} k = m.\ell \quad \text{FOR SOME } \ell \in \mathbb{N}.$$

THIS SHOWS THAT $m \mid (m-1)!$. ASSUME NOW THAT $s=t$. THEN $s^2=m$. SINCE $s \leq m-1$ WE HAVE s IS A FACTOR OF $(m-1)!$. AS $m>4$, WE ALSO NOTE $s^2=m>4$ IMPLIES THAT $s>2$ AND SO $m^2=s.s>2s$. THEN $2s \leq m-1$ AND SO $2s$ IS A FACTOR OF $(m-1)!$. HENCE, s AND $2s$ ARE TWO DIFFERENT FACTORS OF $(m-1)!$ SINCE $s>1$. THEREFORE, WE CAN WRITE

$$(m-1)! = s.\,2s. \prod_{\substack{k=1 \\ k\neq s,\, k\neq 2s}}^{m-1} k = s^2.\,2\prod_{\substack{k=1 \\ k\neq s,\, k\neq 2s}}^{m-1} k = m.\,2.\prod_{\substack{k=1 \\ k\neq s,\, k\neq 2s}}^{m-1} k = m\,\ell$$

FOR SOME $\ell \in \mathbb{N}$. THIS SHOWS THAT $m \mid (m-1)!$. THE RESULT FOLLOWS.

EXERCISE: SHOW THAT ANY INTEGER OF THE FORM 8^m+1, WHERE $m>1$, IS COMPOSITE.

SOLUTION: RECALL WE PROVED IF $k \in \mathbb{N}$ IS AN ODD NUMBER THEN $a+b \mid a^k+b^k$ FOR $a,b \in \mathbb{Z}$. IN PARTICULAR, $a+b \mid a^3+b^3$. SO, IF $a=2^m$ AND $b=1$ WE HAVE $2^m+1 \mid (2^m)^3+1^3$. THAT IS, $2^m+1 \mid 8^m+1$, WHERE $m>1$. NOTICE THAT $2^m+1>1$. SINCE $m>1$ WE ALSO OBSERVE $8^m+1 > 2^m+1$. SO, WE HAVE $1 < 2^m+1 < 8^m+1$. THEN, 2^m+1 IS A NONTRIVIAL DIVISOR OF 8^m+1. WE THEREFORE HAVE 8^m+1 IS COMPOSITE.

EXERCISE: SHOW THAT EVERY INTEGER $m > 11$ CAN BE WRITTEN AS THE SUM OF TWO COMPOSITE NUMBERS.

SOLUTION: LET $m > 11$. SUPPOSE THAT m IS EVEN. THEN, $m = 2k$ FOR SOME $k \in \mathbb{N}$, $k \geq 6$. NOTE THAT $m = 6 + 2k - 6 = 6 + 2(k-3)$. AS $k \geq 6$, WE HAVE $k-3 \geq 3 > 1$ AND SO $2(k-3)$ IS COMPOSITE. SINCE 6 IS COMPOSITE, $m = 6 + 2(k-3)$ IS SUM OF TWO COMPOSITE NUMBERS.

NOW ASSUME THAT m IS ODD. THEN, THERE EXISTS $k \in \mathbb{N}$ SUCH THAT $m = 2k+1$ FOR SOME $k \geq 6$. NOTE THAT, IN THIS CASE, WE CAN WRITE $m = 2k+1 = 2(k-4)+9$. AS $k \geq 6$, $k-4 > 1$ AND SO $2(k-4)$ IS COMPOSITE. SINCE $9 = 3^2$, WE HAVE m IS THE SUM OF TWO COMPOSITE NUMBERS.

EXERCISE: IF $m > 1$ IS AN INTEGER NOT OF THE FORM $6k+3$, PROVE THAT $m^2 + 2^m$ IS COMPOSITE.

SOLUTION: LET $m > 1$ BE AN INTEGER NOT OF THE FORM $6k+3$. THEN, BY THE ALGORITHM DIVISION THEOREM, WE CAN WRITE $m = 6q + r$ FOR SOME $q, r \in \mathbb{Z}$ WITH $r \in \{0, 1, 2, \cancel{3}, 4, 5\}$. THEN, WE OBSERVE

$$m^2 + 2^m = (6q+r)^2 + 2^{6q+r} = 36q^2 + 12qr + r^2 + 2^{6q+r}$$

AS $m > 1$, 2^{6q+r} IS EVEN AND SO $2 \mid (36q^2 + 12qr + 2^{6q+r})$. IF $r \in \{0, 2, 4\}$ THEN $2 \mid r$ WHICH IMPLIES THAT $2 \mid r^2$. WE THUS HAVE $2 \mid (36q^2 + 12qr + 2^{6q+r}) + r^2$ WHICH MEANS THAT $2 \mid (m^2 + 2^m)$. NOTE THAT $m^2 + 2^m > 2^m > 2$ AS $m > 1$. THIS SHOWS THAT 2 IS A NONTRIVIAL DIVISOR OF $m^2 + 2^m$. THEN, $m^2 + 2^m$ IS NOT PRIME. ASSUME NEXT THAT $r \in \{1, 5\}$. NOTE THAT $r^2 - 1 \in \{0, 24\}$ AND SO, $3 \mid (r^2 - 1)$. WE NEXT CLAIM THAT 3 DIVIDES $2^{6q+r} + 1$. TO PROVE

THIS, RECALL $a-b \mid a^n-b^n$ FOR EVERY $a,b\in\mathbb{Z}$, $n\in\mathbb{N}$. SINCE $6q+r$ IS odd WHEN $r\in\{1,5\}$, WE HAVE $2^{6q+r}+1 = 2^{6q+r}-(-1) = 2^{6q+r}-(-1)^{6q+r}$. THEN, $(2-(-1))$ DIVIDES $2^{6q+r}-(-1)^{6q+r}$. THAT IS, $3 \mid (2^{6q+r}+1)$. NOW, WE OBSERVE $m^2+2^m = 36q^2+12qr+r^2+2^{6q+r} = 36q^2+12qr+(r^2-1)+(1+2^{6q+r})$. THEREFORE, SINCE $3\mid(36q^2+12qr)$, $3\mid(r^2-1)$ AND $3\mid(1+2^{6q+r})$ WE HAVE $3\mid m^2+2^m$. NOTE THAT $m^2+2^m > 1+2^1 = 3$ AS $m>1$. SO, 3 IS A NONTRIVIAL DIVISOR OF m^2+2^m. HENCE, m^2+2^m IS COMPOSITE.