

$a \times b = 5$ است که در آن: $a = 5$ و $b = 1$. پس، از تساوی $(3m + 2n)(3n - 2n) = 5 \times 1$ داریم: $3n + 2n = 5$ و $3m - 2n = 1$ (به وضوح مشخص است که $3m - 2n < 3m + 2n$). حال m و n را به دست می آوریم:

$$\begin{cases} 3m + 2n = 5 & m = 1 \\ 3m - 2n = 1 & n = 1 \end{cases} \Rightarrow$$

اکنون این سؤال مطرح می شود که آیا بزرگ ترین عدد اول وجود دارد؟ پاسخ این سؤال را اقلیدس ۲۰۰۰ سال پیش به صورت زیر داده است:

قضیه اقلیدس: مجموعه اعداد اول نامتناهی است. به عبارت دیگر، بی نهایت عدد اول وجود دارد.

با این که بی نهایت عدد اول وجود دارد، توزیع اعداد اول در مجموعه اعداد طبیعی پر رمز و راز است. این اعداد، برخلاف تعریف ساده شان، در میان اعداد طبیعی رشد می کنند و هیچ کس نمی تواند پیش بینی کند که عدد اول بعدی در کجا سبز خواهد شد. در عین حال، واقعیت شگفت انگیز دیگری هم درباره این اعداد وجود دارد: این است که به جز کوچک ترین دو عدد اول یعنی ۲ و ۳، هیچ دو عدد اول دیگری متوالی نیستند و تنها عدد ۲، عدد اول زوج است. بنابراین، همه اعداد اول به غیر از ۲ فرزند و اختلاف دو عدد اول متوالی حداقل برابر ۲ است. اگر اختلاف دو عدد اول برابر ۲ باشد، آن دو عدد اول را «دوقلو» می گویم.

مثال. «۱۱» و «۱۳» و «۱۷» و «۱۹» نمونه هایی از اعداد اول دوقلو هستند.

نکته: هر عدد اول به یکی از صورت های ۲ یا $4k + 1$ یا $4k + 3$ است. زیرا تنها عدد اول زوج، عدد ۲ است و سایر اعداد اول فرزند و اعداد فرد نیز به یکی از صورت های $4k + 1$ یا $4k + 3$ هستند.

به عنوان مثال، عدد اول ۱۷ به صورت $4 \times 4 + 1$ ($k = 4$) یا عدد اول ۲۳ به صورت $4 \times 5 + 3$ ($k = 5$) نوشته می شود.

توجه کنید که عکس مطلب فوق درست نیست. یعنی نمی توان گفت که هر عدد به صورت $4k + 1$ یا $4k + 3$ اول است. مثلاً به ازای $k = 5$ ، $4k + 1$ مساوی ۲۱ است و ۲۱ اول نیست. در واقع $4k + 1$ و $4k + 3$ به ازای بعضی مقادیر

طبیعی k اعداد اول را تولید می کنند. با توجه به نامتناهی بودن مجموعه اعداد اول می توان نتیجه گرفت که بی نهایت عدد اول از نوع $4k + 1$ یا $4k + 3$ وجود دارد.

دیریکله^۱ (۱۸۵۹ - ۱۸۰۵ م) ثابت کرد، اگر a و b نسبت به هم اول باشند، $a + kb$ بی نهایت عدد اول تولید می کند. البته این نکته بدین معنی نیست که $a + kb$ فقط اعداد اول تولید می کند.

اعداد مرسن^۲ (۱۶۴۸ - ۱۵۸۸ م): اعداد به صورت $M_n = 2^n - 1$ را به افتخار کشیش فرانسوی، مارین مرسن، اعداد مرسن نامیده اند. ولی مرسن در زمینه اول بودن این نوع اعداد اظهار نظر نادرستی ارائه کرد. در سال ۱۶۴۴، مرسن اظهار داشت که $M_n = 2^n - 1$ ، به ازای اعداد اول $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ است و به ازای سایر عددهای طبیعی کوچک تر از ۲۵۷ عددی مرکب است.

به اعدادی به شکل $2^n - 1$ که در آن n اول است، اعداد اول مرسن می گویند.

مرسن چند اشتباه داشت. اولاً او به خطا تصور کرد $M_{67} = 2^{67} - 1$ و $M_{257} = 2^{257} - 1$ اول هستند. ثانیاً $M_{11}, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}, M_{89}, M_{113}, M_{127}, M_{157}, M_{199}, M_{313}, M_{347}, M_{431}, M_{439}, M_{487}, M_{509}, M_{599}, M_{719}, M_{811}, M_{983}, M_{1013}, M_{1279}, M_{1549}, M_{1601}, M_{1951}, M_{2161}, M_{2579}, M_{2839}, M_{3631}, M_{4171}, M_{4261}, M_{4369}, M_{4399}, M_{4679}, M_{5461}, M_{6449}, M_{6499}, M_{6607}, M_{6731}, M_{6839}, M_{7681}, M_{7879}, M_{8161}, M_{8581}, M_{8761}, M_{9179}, M_{9679}, M_{9949}, M_{11149}, M_{11257}, M_{11579}, M_{11719}, M_{11857}, M_{11951}, M_{12209}, M_{12271}, M_{12379}, M_{12559}, M_{12577}, M_{12841}, M_{12889}, M_{12947}, M_{13009}, M_{13091}, M_{13139}, M_{13171}, M_{13217}, M_{13297}, M_{13339}, M_{13397}, M_{13451}, M_{13499}, M_{13567}, M_{13627}, M_{13699}, M_{13789}, M_{13841}, M_{13907}, M_{13979}, M_{14039}, M_{14107}, M_{14171}, M_{14243}, M_{14317}, M_{14399}, M_{14471}, M_{14543}, M_{14617}, M_{14699}, M_{14771}, M_{14843}, M_{14917}, M_{14999}, M_{15071}, M_{15143}, M_{15217}, M_{15299}, M_{15371}, M_{15443}, M_{15517}, M_{15599}, M_{15671}, M_{15743}, M_{15817}, M_{15899}, M_{15971}, M_{16043}, M_{16117}, M_{16199}, M_{16271}, M_{16343}, M_{16417}, M_{16499}, M_{16571}, M_{16643}, M_{16717}, M_{16799}, M_{16871}, M_{16943}, M_{17017}, M_{17099}, M_{17171}, M_{17243}, M_{17317}, M_{17399}, M_{17471}, M_{17543}, M_{17617}, M_{17699}, M_{17771}, M_{17843}, M_{17917}, M_{17999}, M_{18071}, M_{18143}, M_{18217}, M_{18299}, M_{18371}, M_{18443}, M_{18517}, M_{18599}, M_{18671}, M_{18743}, M_{18817}, M_{18899}, M_{18971}, M_{19043}, M_{19117}, M_{19199}, M_{19271}, M_{19343}, M_{19417}, M_{19499}, M_{19571}, M_{19643}, M_{19717}, M_{19799}, M_{19871}, M_{19943}, M_{20017}, M_{20099}, M_{20171}, M_{20243}, M_{20317}, M_{20399}, M_{20471}, M_{20543}, M_{20617}, M_{20699}, M_{20771}, M_{20843}, M_{20917}, M_{20999}, M_{21071}, M_{21143}, M_{21217}, M_{21299}, M_{21371}, M_{21443}, M_{21517}, M_{21599}, M_{21671}, M_{21743}, M_{21817}, M_{21899}, M_{21971}, M_{22043}, M_{22117}, M_{22199}, M_{22271}, M_{22343}, M_{22417}, M_{22499}, M_{22571}, M_{22643}, M_{22717}, M_{22799}, M_{22871}, M_{22943}, M_{23017}, M_{23099}, M_{23171}, M_{23243}, M_{23317}, M_{23399}, M_{23471}, M_{23543}, M_{23617}, M_{23699}, M_{23771}, M_{23843}, M_{23917}, M_{23999}, M_{24071}, M_{24143}, M_{24217}, M_{24299}, M_{24371}, M_{24443}, M_{24517}, M_{24599}, M_{24671}, M_{24743}, M_{24817}, M_{24899}, M_{24971}, M_{25043}, M_{25117}, M_{25199}, M_{25271}, M_{25343}, M_{25417}, M_{25499}, M_{25571}, M_{25643}, M_{25717}, M_{25799}, M_{25871}, M_{25943}, M_{26017}, M_{26099}, M_{26171}, M_{26243}, M_{26317}, M_{26399}, M_{26471}, M_{26543}, M_{26617}, M_{26699}, M_{26771}, M_{26843}, M_{26917}, M_{26999}, M_{27071}, M_{27143}, M_{27217}, M_{27299}, M_{27371}, M_{27443}, M_{27517}, M_{27599}, M_{27671}, M_{27743}, M_{27817}, M_{27899}, M_{27971}, M_{28043}, M_{28117}, M_{28199}, M_{28271}, M_{28343}, M_{28417}, M_{28499}, M_{28571}, M_{28643}, M_{28717}, M_{28799}, M_{28871}, M_{28943}, M_{29017}, M_{29099}, M_{29171}, M_{29243}, M_{29317}, M_{29399}, M_{29471}, M_{29543}, M_{29617}, M_{29699}, M_{29771}, M_{29843}, M_{29917}, M_{29999}, M_{30071}, M_{30143}, M_{30217}, M_{30299}, M_{30371}, M_{30443}, M_{30517}, M_{30599}, M_{30671}, M_{30743}, M_{30817}, M_{30899}, M_{30971}, M_{31043}, M_{31117}, M_{31199}, M_{31271}, M_{31343}, M_{31417}, M_{31499}, M_{31571}, M_{31643}, M_{31717}, M_{31799}, M_{31871}, M_{31943}, M_{32017}, M_{32099}, M_{32171}, M_{32243}, M_{32317}, M_{32399}, M_{32471}, M_{32543}, M_{32617}, M_{32699}, M_{32771}, M_{32843}, M_{32917}, M_{32999}, M_{33071}, M_{33143}, M_{33217}, M_{33299}, M_{33371}, M_{33443}, M_{33517}, M_{33599}, M_{33671}, M_{33743}, M_{33817}, M_{33899}, M_{33971}, M_{34043}, M_{34117}, M_{34199}, M_{34271}, M_{34343}, M_{34417}, M_{34499}, M_{34571}, M_{34643}, M_{34717}, M_{34799}, M_{34871}, M_{34943}, M_{35017}, M_{35099}, M_{35171}, M_{35243}, M_{35317}, M_{35399}, M_{35471}, M_{35543}, M_{35617}, M_{35699}, M_{35771}, M_{35843}, M_{35917}, M_{35999}, M_{36071}, M_{36143}, M_{36217}, M_{36299}, M_{36371}, M_{36443}, M_{36517}, M_{36599}, M_{36671}, M_{36743}, M_{36817}, M_{36899}, M_{36971}, M_{37043}, M_{37117}, M_{37199}, M_{37271}, M_{37343}, M_{37417}, M_{37499}, M_{37571}, M_{37643}, M_{37717}, M_{37799}, M_{37871}, M_{37943}, M_{38017}, M_{38099}, M_{38171}, M_{38243}, M_{38317}, M_{38399}, M_{38471}, M_{38543}, M_{38617}, M_{38699}, M_{38771}, M_{38843}, M_{38917}, M_{38999}, M_{39071}, M_{39143}, M_{39217}, M_{39299}, M_{39371}, M_{39443}, M_{39517}, M_{39599}, M_{39671}, M_{39743}, M_{39817}, M_{39899}, M_{39971}, M_{40043}, M_{40117}, M_{40199}, M_{40271}, M_{40343}, M_{40417}, M_{40499}, M_{40571}, M_{40643}, M_{40717}, M_{40799}, M_{40871}, M_{40943}, M_{41017}, M_{41099}, M_{41171}, M_{41243}, M_{41317}, M_{41399}, M_{41471}, M_{41543}, M_{41617}, M_{41699}, M_{41771}, M_{41843}, M_{41917}, M_{41999}, M_{42071}, M_{42143}, M_{42217}, M_{42299}, M_{42371}, M_{42443}, M_{42517}, M_{42599}, M_{42671}, M_{42743}, M_{42817}, M_{42899}, M_{42971}, M_{43043}, M_{43117}, M_{43199}, M_{43271}, M_{43343}, M_{43417}, M_{43499}, M_{43571}, M_{43643}, M_{43717}, M_{43799}, M_{43871}, M_{43943}, M_{44017}, M_{44099}, M_{44171}, M_{44243}, M_{44317}, M_{44399}, M_{44471}, M_{44543}, M_{44617}, M_{44699}, M_{44771}, M_{44843}, M_{44917}, M_{44999}, M_{45071}, M_{45143}, M_{45217}, M_{45299}, M_{45371}, M_{45443}, M_{45517}, M_{45599}, M_{45671}, M_{45743}, M_{45817}, M_{45899}, M_{45971}, M_{46043}, M_{46117}, M_{46199}, M_{46271}, M_{46343}, M_{46417}, M_{46499}, M_{46571}, M_{46643}, M_{46717}, M_{46799}, M_{46871}, M_{46943}, M_{47017}, M_{47099}, M_{47171}, M_{47243}, M_{47317}, M_{47399}, M_{47471}, M_{47543}, M_{47617}, M_{47699}, M_{47771}, M_{47843}, M_{47917}, M_{47999}, M_{48071}, M_{48143}, M_{48217}, M_{48299}, M_{48371}, M_{48443}, M_{48517}, M_{48599}, M_{48671}, M_{48743}, M_{48817}, M_{48899}, M_{48971}, M_{49043}, M_{49117}, M_{49199}, M_{49271}, M_{49343}, M_{49417}, M_{49499}, M_{49571}, M_{49643}, M_{49717}, M_{49799}, M_{49871}, M_{49943}, M_{50017}, M_{50099}, M_{50171}, M_{50243}, M_{50317}, M_{50399}, M_{50471}, M_{50543}, M_{50617}, M_{50699}, M_{50771}, M_{50843}, M_{50917}, M_{50999}, M_{51071}, M_{51143}, M_{51217}, M_{51299}, M_{51371}, M_{51443}, M_{51517}, M_{51599}, M_{51671}, M_{51743}, M_{51817}, M_{51899}, M_{51971}, M_{52043}, M_{52117}, M_{52199}, M_{52271}, M_{52343}, M_{52417}, M_{52499}, M_{52571}, M_{52643}, M_{52717}, M_{52799}, M_{52871}, M_{52943}, M_{53017}, M_{53099}, M_{53171}, M_{53243}, M_{53317}, M_{53399}, M_{53471}, M_{53543}, M_{53617}, M_{53699}, M_{53771}, M_{53843}, M_{53917}, M_{53999}, M_{54071}, M_{54143}, M_{54217}, M_{54299}, M_{54371}, M_{54443}, M_{54517}, M_{54599}, M_{54671}, M_{54743}, M_{54817}, M_{54899}, M_{54971}, M_{55043}, M_{55117}, M_{55199}, M_{55271}, M_{55343}, M_{55417}, M_{55499}, M_{55571}, M_{55643}, M_{55717}, M_{55799}, M_{55871}, M_{55943}, M_{56017}, M_{56099}, M_{56171}, M_{56243}, M_{56317}, M_{56399}, M_{56471}, M_{56543}, M_{56617}, M_{56699}, M_{56771}, M_{56843}, M_{56917}, M_{56999}, M_{57071}, M_{57143}, M_{57217}, M_{57299}, M_{57371}, M_{57443}, M_{57517}, M_{57599}, M_{57671}, M_{57743}, M_{57817}, M_{57899}, M_{57971}, M_{58043}, M_{58117}, M_{58199}, M_{58271}, M_{58343}, M_{58417}, M_{58499}, M_{58571}, M_{58643}, M_{58717}, M_{58799}, M_{58871}, M_{58943}, M_{59017}, M_{59099}, M_{59171}, M_{59243}, M_{59317}, M_{59399}, M_{59471}, M_{59543}, M_{59617}, M_{59699}, M_{59771}, M_{59843}, M_{59917}, M_{59999}, M_{60071}, M_{60143}, M_{60217}, M_{60299}, M_{60371}, M_{60443}, M_{60517}, M_{60599}, M_{60671}, M_{60743}, M_{60817}, M_{60899}, M_{60971}, M_{61043}, M_{61117}, M_{61199}, M_{61271}, M_{61343}, M_{61417}, M_{61499}, M_{61571}, M_{61643}, M_{61717}, M_{61799}, M_{61871}, M_{61943}, M_{62017}, M_{62099}, M_{62171}, M_{62243}, M_{62317}, M_{62399}, M_{62471}, M_{62543}, M_{62617}, M_{62699}, M_{62771}, M_{62843}, M_{62917}, M_{62999}, M_{63071}, M_{63143}, M_{63217}, M_{63299}, M_{63371}, M_{63443}, M_{63517}, M_{63599}, M_{63671}, M_{63743}, M_{63817}, M_{63899}, M_{63971}, M_{64043}, M_{64117}, M_{64199}, M_{64271}, M_{64343}, M_{64417}, M_{64499}, M_{64571}, M_{64643}, M_{64717}, M_{64799}, M_{64871}, M_{64943}, M_{65017}, M_{65099}, M_{65171}, M_{65243}, M_{65317}, M_{65399}, M_{65471}, M_{65543}, M_{65617}, M_{65699}, M_{65771}, M_{65843}, M_{65917}, M_{65999}, M_{66071}, M_{66143}, M_{66217}, M_{66299}, M_{66371}, M_{66443}, M_{66517}, M_{66599}, M_{66671}, M_{66743}, M_{66817}, M_{66899}, M_{66971}, M_{67043}, M_{67117}, M_{67199}, M_{67271}, M_{67343}, M_{67417}, M_{67499}, M_{67571}, M_{67643}, M_{67717}, M_{67799}, M_{67871}, M_{67943}, M_{68017}, M_{68099}, M_{68171}, M_{68243}, M_{68317}, M_{68399}, M_{68471}, M_{68543}, M_{68617}, M_{68699}, M_{68771}, M_{68843}, M_{68917}, M_{68999}, M_{69071}, M_{69143}, M_{69217}, M_{69299}, M_{69371}, M_{69443}, M_{69517}, M_{69599}, M_{69671}, M_{69743}, M_{69817}, M_{69899}, M_{69971}, M_{70043}, M_{70117}, M_{70199}, M_{70271}, M_{70343}, M_{70417}, M_{70499}, M_{70571}, M_{70643}, M_{70717}, M_{70799}, M_{70871}, M_{70943}, M_{71017}, M_{71099}, M_{71171}, M_{71243}, M_{71317}, M_{71399}, M_{71471}, M_{71543}, M_{71617}, M_{71699}, M_{71771}, M_{71843}, M_{71917}, M_{71999}, M_{72071}, M_{72143}, M_{72217}, M_{72299}, M_{72371}, M_{72443}, M_{72517}, M_{72599}, M_{72671}, M_{72743}, M_{72817}, M_{72899}, M_{72971}, M_{73043}, M_{73117}, M_{73199}, M_{73271}, M_{73343}, M_{73417}, M_{73499}, M_{73571}, M_{73643}, M_{73717}, M_{73799}, M_{73871}, M_{73943}, M_{74017}, M_{74099}, M_{74171}, M_{74243}, M_{74317}, M_{74399}, M_{74471}, M_{74543}, M_{74617}, M_{74699}, M_{74771}, M_{74843}, M_{74917}, M_{74999}, M_{75071}, M_{75143}, M_{75217}, M_{75299}, M_{75371}, M_{75443}, M_{75517}, M_{75599}, M_{75671}, M_{75743}, M_{75817}, M_{75899}, M_{75971}, M_{76043}, M_{76117}, M_{76199}, M_{76271}, M_{76343}, M_{76417}, M_{76499}, M_{76571}, M_{76643}, M_{76717}, M_{76799}, M_{76871}, M_{76943}, M_{77017}, M_{77099}, M_{77171}, M_{77243}, M_{77317}, M_{77399}, M_{77471}, M_{77543}, M_{77617}, M_{77699}, M_{77771}, M_{77843}, M_{77917}, M_{77999}, M_{78071}, M_{78143}, M_{78217}, M_{78299}, M_{78371}, M_{78443}, M_{78517}, M_{78599}, M_{78671}, M_{78743}, M_{78817}, M_{78899}, M_{78971}, M_{79043}, M_{79117}, M_{79199}, M_{79271}, M_{79343}, M_{79417}, M_{79499}, M_{79571}, M_{79643}, M_{79717}, M_{79799}, M_{79871}, M_{79943}, M_{80017}, M_{80099}, M_{80171}, M_{80243}, M_{80317}, M_{80399}, M_{80471}, M_{80543}, M_{80617}, M_{80699}, M_{80771}, M_{80843}, M_{80917}, M_{80999}, M_{81071}, M_{81143}, M_{81217}, M_{81299}, M_{81371}, M_{81443}, M_{81517}, M_{81599}, M_{81671}, M_{81743}, M_{81817}, M_{81899}, M_{81971}, M_{82043}, M_{82117}, M_{82199}, M_{82271}, M_{82343}, M_{82417}, M_{82499}, M_{82571}, M_{82643}, M_{82717}, M_{82799}, M_{82871}, M_{82943}, M_{83017}, M_{83099}, M_{83171}, M_{83243}, M_{83317}, M_{83399}, M_{83471}, M_{83543}, M_{83617}, M_{83699}, M_{83771}, M_{83843}, M_{83917}, M_{83999}, M_{84071}, M_{84143}, M_{84217}, M_{84299}, M_{84371}, M_{84443}, M_{84517}, M_{84599}, M_{84671}, M_{84743}, M_{84817}, M_{84899}, M_{84971}, M_{85043}, M_{85117}, M_{85199}, M_{85271}, M_{85343}, M_{85417}, M_{85499}, M_{85571}, M_{85643}, M_{85717}, M_{85799}, M_{85871}, M_{85943}, M_{86017}, M_{86099}, M_{86171}, M_{86243}, M_{86317}, M_{86399}, M_{86471}, M_{86543}, M_{86617}, M_{86699}, M_{86771}, M_{86843}, M_{86917}, M_{86999}, M_{87071}, M_{87143}, M_{87217}, M_{87299}, M_{87371}, M_{87443}, M_{87517}, M_{87599}, M_{87671}, M_{87743}, M_{87817}, M_{87899}, M_{87971}, M_{88043}, M_{88117}, M_{88199}, M_{88271}, M_{88343}, M_{88417}, M_{88499}, M_{88571}, M_{88643}, M_{88717}, M_{88799}, M_{88871}, M_{88943}, M_{89017}, M_{89099}, M_{89171}, M_{89243}, M_{89317}, M_{89399}, M_{89471}, M_{89543}, M_{89617}, M_{89699}, M_{89771}, M_{89843}, M_{89917}, M_{89999}, M_{90071}, M_{90143}, M_{90217}, M_{90299}, M_{90371}, M_{90443}, M_{90517}, M_{90599}, M_{90671}, M_{90743}, M_{90817}, M_{90899}, M_{90971}, M_{91043}, M_{91117}, M_{91199}, M_{91271}, M_{91343}, M_{91417}, M_{91499}, M_{91571}, M_{91643}, M_{91717}, M_{91799}, M_{91871}, M_{91943}, M_{92017}, M_{92099}, M_{92171}, M_{92243}, M_{92317}, M_{92399}, M_{92471}, M_{92543}, M_{92617}, M_{92699}, M_{92771}, M_{92843}, M_{92917}, M_{92999}, M_{93071}, M_{93143}, M_{93217}, M_{93299}, M_{93371}, M_{93443}, M_{93517}, M_{93599}, M_{93671}, M_{93743}, M_{93817}, M_{93899}, M_{93971}, M_{94043}, M_{94117}, M_{94199}, M_{94271}, M_{94343}, M_{94417}, M_{94499}, M_{94571}, M_{94643}, M_{94717}, M_{94799}, M_{94871}, M_{94943}, M_{95017}, M_{95099}, M_{95171}, M_{95243}, M_{95317}, M_{95399}, M_{95471}, M_{95543}, M_{95617}, M_{95699}, M_{95771}, M_{95843}, M_{95917}, M_{95999}, M_{96071}, M_{96143}, M_{96217}, M_{96299}, M_{96371}, M_{96443}, M_{96517}, M_{96599}, M_{96671}, M_{96743}, M_{96817}, M_{96899}, M_{96971}, M_{97043}, M_{97117}, M_{97199}, M_{97271}, M_{97343}, M_{97417}, M_{97499}, M_{97571}, M_{97643}, M_{97717}, M_{97799}, M_{97871}, M_{97943}, M_{98017}, M_{98099}, M_{98171}, M_{98243}, M_{98317}, M_{98399}, M_{98471}, M_{98543}, M_{98617}, M_{98699}, M_{98771}, M_{98843}, M_{98917}, M_{98999}, M_{99071}, M_{99143}, M_{99217}, M_{99299}, M_{99371}, M_{99443}, M_{99517}, M_{99599}, M_{99671}, M_{99743}, M_{99817}, M_{99899}, M_{99971}, M_{100043}, M_{100117}, M_{100199}, M_{100271}, M_{100343}, M_{100417}, M_{100499}, M_{100571}, M_{100643}, M_{100717}, M_{100799}, M_{100871}, M_{100943}, M_{101017}, M_{101099}, M_{101171}, M_{101243}, M_{101317}, M_{101399}, M_{101471}, M_{101543}, M_{101617}, M_{101699}, M_{101771}, M_{101843}, M_{101917}, M_{101999}, M_{102071}, M_{102143}, M_{102217}, M_{102299}, M_{102371}, M_{102443}, M_{102517}, M_{102599}, M_{102671}, M_{102743}, M_{102817}, M_{102899}, M_{102971}, M_{103043}, M_{103117}, M_{103199}, M_{103271}, M_{103343}, M_{103417}, M_{103499}, M_{103571}, M_{103643}, M_{103717}, M_{103799}, M_{103871}, M_{103943}, M_{104017}, M_{104099}, M_{104171}, M_{104243}, M_{104317}, M_{104399}, M_{104471}, M_{104543}, M_{104617}, M_{104699}, M_{104771}, M_{104843}, M_{104917}, M_{104999}, M_{105071}, M_{105143}, M_{105217}, M_{105299}, M_{105371}, M_{105443}, M_{105517}, M_{105599}, M_{105671}, M_{105743}, M_{105817}, M_{105899}, M_{105971}, M_{106043}, M_{106117}, M_{106199}, M_{106271}, M_{106343}, M_{106417}, M_{106499}, M_{10657$

اعداد اول بین ۱ و ۱۰۰۰ در جدول زیر آمده‌اند:

۲	۳	۵	۷	۱۱	۱۳	۱۷	۱۹	۲۳
۲۹	۳۱	۳۷	۴۱	۴۳	۴۷	۵۳	۵۹	۶۷
۷۱	۷۳	۷۹	۸۳	۸۹	۹۷	۱۰۱	۱۰۳	۱۰۷
۱۱۳	۱۲۷	۱۳۱	۱۳۷	۱۳۹	۱۴۹	۱۵۱	۱۵۷	۱۶۳
۱۷۳	۱۷۹	۱۸۱	۱۹۱	۱۹۳	۱۹۷	۱۹۹	۲۱۱	۲۲۳
۲۲۹	۲۳۳	۲۳۹	۲۴۱	۲۵۱	۲۵۷	۲۶۳	۲۶۹	۲۷۱
۲۸۱	۲۸۳	۲۹۳	۳۰۷	۳۱۱	۳۱۳	۳۱۷	۳۳۱	۳۳۷
۳۴۹	۳۵۳	۳۵۹	۳۶۷	۳۷۳	۳۷۹	۳۸۳	۳۸۹	۳۹۷
۴۰۹	۴۱۹	۴۲۱	۴۳۱	۴۳۳	۴۳۹	۴۴۳	۴۴۹	۴۵۷
۴۶۳	۴۶۷	۴۷۹	۴۸۷	۴۹۱	۴۹۹	۵۰۳	۵۰۹	۵۲۱
۵۲۳	۵۲۹	۵۳۹	۵۴۷	۵۵۷	۵۶۳	۵۶۹	۵۷۱	۵۷۷
۵۸۷	۵۹۳	۵۹۹	۶۰۷	۶۱۳	۶۱۷	۶۱۹	۶۳۱	۶۴۱
۶۴۳	۶۴۷	۶۵۳	۶۶۱	۶۷۳	۶۷۷	۶۸۳	۶۹۱	۷۰۱
۷۰۹	۷۱۹	۷۲۱	۷۳۳	۷۳۹	۷۴۳	۷۵۱	۷۵۷	۷۶۱
۷۶۹	۷۷۳	۷۸۷	۷۹۷	۸۰۹	۸۱۱	۸۲۱	۸۲۳	۸۲۷
۸۲۹	۸۳۹	۸۵۳	۸۵۷	۸۶۳	۸۶۷	۸۷۳	۸۸۳	۸۸۷
۸۸۷	۸۹۷	۹۰۷	۹۱۱	۹۱۹	۹۲۹	۹۳۷	۹۴۱	۹۴۷
۹۴۷	۹۵۳	۹۶۷	۹۷۱	۹۷۷	۹۸۳	۹۹۱	۹۹۷	(۱۰۰۹)

اول بودن $2^n - 1$ است.

البته عکس مسأله فوق درست نیست. به عنوان مثال،

$2^{11} - 1 = 2047$ که بر ۲۳ بخش پذیر است، اول نیست.

عدد فرما: $F_n = 2^{2^n} - 1$ (۱۶۶۵-۱۶۰۱ م)

هر عدد فرما، عددی است به صورت $F_n = 2^{2^n} - 1$ ($n \geq 0$).

اگر F_n اول باشد، آن را عدد اول فرما می‌گویند.

مسأله. اگر $2^m + 1$ اول باشد، نشان دهید: $m = 2^n$.

اثبات. (برهان خلف) فرض کنید m توانی از ۲ نیست؛ یعنی:

$2^m \neq 2^n$. لذا m مقسوم علیه فردی مانند $2k+1$ دارد که از یک بزرگ‌تر است. بنابراین:

$$M = (2k+1)L; (k, L \in \mathbb{N})$$

حال داریم:

$$2^m + 1 = 2^{(2k+1)L} + 1 = (2^L)^{(2k+1)} + 1 = (2^L + 1)((2^L)^{(2k+1-1)} - 2^L(2k-1) + \dots + 1)$$

یعنی $2^m + 1$ تجزیه غیربدهی دارد، پس اول نیست که این خلاف فرض است. پس نتیجه می‌گیریم که شرط لازم برای اول بودن $2^m + 1$ ، این است که $m = 2^n$ باشد.

فرما مشاهده کرد که:

$$F_2 = 2^{2^2} + 1 = 17, F_3 = 2^{2^3} + 1 = 257, F_4 = 2^{2^4} + 1 = 65537$$

خطا تصور کرد که همه F_n ها اولند.

در سال ۱۷۳۲، اولر نشان داد که F_5 بر ۶۴۱ بخش پذیر است.

$$F_5 = 2^{2^5} + 1 = 4294967297$$

بنابراین خط بطلانی بر ادعای فرما کشید. البته ممکن است برای ما چنین عددی بزرگ جلوه نکند، ولی در زمان فرما به علت محدودیت ابزار محاسبه‌های بزرگ، تشخیص

اول بودن این عدد کاری بسیار دشوار بود.

اکنون ثابت شده است که به ازای همه اعداد طبیعی $21 \leq n \leq 5$ ، F_n مرکب است.

ریاضیدانان اعداد اول را مانند بلوک‌های ساختمانی می‌دانند که همه اعداد از آن‌ها ساخته شده‌اند. به همین دلیل، سالیان درازی است که ریاضیدانان را شیفته خود ساخته و فکر آن‌ها را مشغول کرده‌اند.

زیرنویس

1. Dirichlet
2. Mersenne
3. <http://www-gap.dcs.St-And.ac.uk/~History/MistTopics/Prime-numbers.html>
4. Fermat

منابع

1. Burton, David M. Elementary Number Theory
۲. نظریه اعداد. سیدحسین سید موسوی و شمس‌الدین انوار.

شماره ۴۷