Writing a Number as a Sum of Two Squares

When can an integer $n \geqslant 1$ be written as a sum of two squares? We certainly require $n \not\equiv 3 \mod 4$; and if the prime factorization of n is known, say

$$n = \prod_p p^{e_p}$$

(as a product over all primes p, with exponents $e_p \geqslant 0$) then the complete characterization is as follows. (The *squarefree part of* n is the largest divisor of n which is not divisible by any square > 1.)

Theorem 1. An integer $n \geqslant 1$ (factored as above) is expressible as a sum of two integer squares, iff e_p is even whenever $p \equiv 3 \mod 4$. Equivalently, n is a sum of two squares iff its squarefree part has no prime divisor $\equiv 3 \mod 4$.

For example, suppose we want to write $92250 = 2{\cdot}3^2{\cdot}5^3{\cdot}41$ as a sum of squares. The Theorem says this is possible since the prime 3 has an even exponent 2. Rewrite

$$92250 = 15^2{\cdot}2{\cdot}5{\cdot}41$$

where the squarefree part of 92250 is evidently $2{\cdot}5{\cdot}41$, which has no prime divisor $\equiv 3 \mod 4$. Since

$$2 = |1+i|^2 = 1^2+1^2, \quad 5 = |2+i|^2 = 2^2+1^2, \quad 41 = |4+5i|^2 = 4^2+5^2,$$

we have $92250 = |z|^2$ where

$$z = 15(1+i)(2+i)(4+5i) = -165+255i,$$

i.e.

$$92250 = 165^2 + 255^2.$$

(Different solutions are obtained if we replace $1+i$ by $1-i$; and $2+i$ by $2-i$ or $1+2i$ or $1-2i$, etc.) It should be evident from our example that one direction (the 'if' part)

of Theorem 1 follows if we can write every prime $p \equiv 1 \mod 4$ as a sum of two squares. Thus we first prove

Theorem 2. Every prime $p \equiv 1 \mod 4$ is expressible as a sum of two integer squares.

Our proof of Theorem 2 is constructive: Given a prime $p \equiv 1 \mod 4$, we actually present an algorithm for writing p as a sum of two integer squares. The first step is to solve an easier problem: find integers a and b such that $a^2 + b^2$ is a *multiple* of p. This is easily solved: Take $b = 1$. Since $p \equiv 1 \mod 4$, there exists an integer a such that $a^2 \equiv -1 \bmod p$. (To find such an integer a, let c be an integer not divisible by p, and take $a \equiv c^{(p-1)/4}$. Then

$$a^2 \equiv c^{(p-1)/2} \equiv \begin{cases} 1 \mod p, & \text{if } \left(\frac{c}{p}\right) = 1; \\ -1 \mod p, & \text{if } \left(\frac{c}{p}\right) = -1. \end{cases}$$

Half of the time we are in the first case, with an immediate success; otherwise try a different value of c (selected randomly from $\mathbb{F}_p^\times$) and repeat. In practice only a few tries are required to obtain a success; for example, 99.9% of the time, at most 10 tries are required (just as ten flips of an unbiased coin will yield at least one head, 99.9% of the time).

Thus we have somehow managed to find integers a, b, m such that $a^2 + b^2 = mp$. The next step is to iteratively express smaller and smaller multiples of p in the required form (as a sum of two squares) until p itself is expressed as a sum of two squares. To this end, we might as well assume $a, b \in \left(-\frac{p}{2}, \frac{p}{2}\right)$; otherwise subtract an integer multiple of p from a, and from b, to get $\widetilde{a} = a - kp \in \left(-\frac{p}{2}, \frac{p}{2}\right)$ and $\widetilde{b} = b - \ell p \in \left(-\frac{p}{2}, \frac{p}{2}\right)$. In particular we now have

$$(1) \qquad a^2 + b^2 = mp; \quad -\tfrac{p}{2} < a, b < \tfrac{p}{2}; \quad 1 \leqslant m < \tfrac{p}{2}.$$

Of course if $m = 1$ then we are done. So assume $m \geqslant 2$, and subtract multiples of m from a and b to obtain

$$a' = a - rm \in \left[-\tfrac{m}{2}, \tfrac{m}{2}\right], \quad b' = b - sm \in \left[-\tfrac{m}{2}, \tfrac{m}{2}\right].$$

We now work in the *ring of Gaussian integers* $\mathbb{Z}[i] = \{u + vi : u, v \in \mathbb{Z}\}$ where $i = \sqrt{-1}$. Set $\alpha = a + bi$, $\beta = a' + b'i$. Recall that $\overline{\alpha} = a - bi$, so that $\alpha\overline{\alpha} = a^2 + b^2 = mp$. Since $\beta \equiv \alpha \bmod m$, we have

$$\alpha\overline{\beta} \equiv \alpha\overline{\alpha} \equiv mp \equiv 0 \mod m;$$

therefore $\alpha\overline{\beta} = m\gamma$ for some $\gamma \in \mathbb{Z}[i]$. Now

$$m^2|\gamma|^2 = m^2\gamma\overline{\gamma} = (\alpha\overline{\beta})(\overline{\alpha}\beta) = (\alpha\overline{\alpha})(\beta\overline{\beta}) = mp\beta\overline{\beta}.$$

Again using $\beta \equiv \alpha \mod m$, we have $\beta\overline{\beta} \equiv \alpha\overline{\alpha} = mp \equiv 0 \mod m$; thus $\beta\overline{\beta} = mm'$ for some integer $m' \geqslant 0$, whence

$$m^2\gamma\overline{\gamma} = m^2m'p,$$

i.e.

$$\gamma\overline{\gamma} = m'p.$$

To compare m' with m, note that $mm' = \beta\overline{\beta} = (a')^2 + (b')^2 \leqslant \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = \frac{m^2}{2}$, i.e. $0 \leqslant m' \leqslant \frac{m}{2}$. If $m' = 0$ then $|\beta|^2 = 0$ so $a' = b' = 0$, i.e. both a and b are multiples of m; but then $mp = |\alpha^2| = a^2 + b^2$ is divisible by m^2, so that m divides p. This is impossible since $2 \leqslant m < \frac{p}{2}$. So actually $1 \leqslant m' \leqslant \frac{m}{2}$, and we have succeeded in descending from mp to $m'p$ as a sum of two squares. This proves Theorem 2.

We demonstrate our algorithm using the prime $p = 9521 \equiv 1 \mod 4$. We see that $\left(\frac{3}{9521}\right) = -1$ and $3^{(9521-1)/4} \equiv 2140 \mod p$, so take

- $\alpha_1 = 2140{+}i,\ |\alpha_1|^2 = 481p,\ \beta_1 = \alpha_1{-}481{\cdot}4 = 216{+}i,\ \gamma_1 = \alpha_1\overline{\beta_1}/481 = 961{-}4i$;
- $\alpha_2 = 961{-}4i,\ |\alpha_2|^2 = 97p,\ \beta_2 = \alpha_2{-}97{\cdot}10 = -9{-}4i,\ \gamma_2 = \alpha_2\overline{\beta_2}/97 = -89{+}40i$;
- $\alpha_3 = -89{+}40i,\ |\alpha_2|^2 = p$.

The desired solution $9521 = 89^2 + 40^2$ is obtained after only 3 iterations of our descent algorithm.

We remark that the solution in Theorem 2 is essentially unique; for example the only integer solutions of $9521 = a^2 + b^2$ are given by $(a, b) = (\pm 89, \pm 40)$ or $(\pm 40, \pm 89)$. (We see that there are eight solutions in all; but they are all trivial modifications of the single solution $(89, 40)$.)

The *descent algorithm* is given in Chapter 24 of our textbook (which however uses ad hoc identities in place of our arithmetic of $\mathbb{Z}[i]$). The descent procedure can also be used to show that the solution to Theorem 2 is essentially unique (in the sense described above), and to show the other direction of Theorem 1 (the 'only if' direction).

The attached Maple worksheet demonstrates the descent algorithm for the smallest 101-digit prime that is congruent to 1 mod 4.

Here is a MAPLE implementation of the descent algorithm for writing a prime (congruent to 1 mod 4) as a sum of two squares.

We demonstrate using the first prime p after a googol that is congruent to 1 mod 4.

```
> p:=nextprime(10^100);
```

$$p := 10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000267 \quad (1$$

```
> p mod 4;
```

$$3 \quad (2$$

```
> p:=nextprime(p);
```

$$p := 10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000949 \quad (3$$

```
> p mod 4;
```

$$1 \quad (4$$

We want to write p as a sum of two squares. First choose a and b such that $a^2 + b^2$. We can take $b = 1$ and $a = c^{\frac{p-1}{4}} \bmod p$ where c is any nonsquare mod p:

```
> a:=2&^((p-1)/4) mod p;
> b:=1;
> m:=(a^2+b^2)/p;
```

$$a := 542052982664259487393800458002474851111791003816425426894553006975641057766599557255252142019678301 4$$

$$b := 1$$

$$m := 293821436015219996368442559739089062431561437341731869152874844356291335699442981883740046713867115 3 \quad (5$$

I tried $c = 2$ and was lucky. Because exactly half of the nonzero integers mod p are nonsquares, there is a 50% chance that the first value of c tried won't give a mod p. In this case try new values of c until one is found that works.

The following procedure performs the *descent step*: Given a pair a, b such that $a^2 + b^2 = m\,p$ with $m > 1$, it finds a new pair a, b such that $a^2 + b^2 = mp$ with a *smaller* value of m.

```
> descend:=proc()
>    global a,b,m: local alpha,beta,gamma,a1,b1:
>    alpha:=a+b*I:
>    m:=alpha*conjugate(alpha)/p:
>    a1:=a mod m:
```

```
>    if a1>m/2 then a1:=a1-m: fi:
>    b1:=b mod m:
>    if b1>m/2 then b1:=b1-m: fi:
>    beta:=a1+b1*I;
>    gamma:=simplify(alpha*conjugate(beta)/m):
>    a:=Re(gamma):
>    b:=Im(gamma):
>    m:=gamma*conjugate(gamma)/p:
>    printf("a^2 + b^2 = m*p where m=%d\n",m);
>    end:
```

Perform the descent step until we reach $m = 1$:

```
> while m>1 do descend(); od;
a^2 + b^2 = m*p where m=
70738134038420358985684069464568452790817341012257690332873495226011117313736985139516187767553505
a^2 + b^2 = m*p where m=
85962268797774491428616170992866821801527388090249854833996423789316521033837756930286908214377 3
a^2 + b^2 = m*p where m=
17717360590185618047336311704459684516703352612854209461253553444392865787856077622674004489437
a^2 + b^2 = m*p where m=
13661435813078928480671194584576311871129105965558173708546326206859094833197129938155680660 00
a^2 + b^2 = m*p where m=
30601115875513997073222749907593768844938670898856114212551527889050171182137145160280643747 7
a^2 + b^2 = m*p where m=
71899872147511842140396758298065660936563219920626996389088702824784385679435039564867293844
a^2 + b^2 = m*p where m=
71862905943072819603721647877944780325203980910199627584994239046717147991763840420981031 25
a^2 + b^2 = m*p where m=
78679846108336085786417714656734825684975575476598746779247848316889131982510469101850912 0
a^2 + b^2 = m*p where m=
16709888419281884970823879859009629163666163653399907346594578232012003617964614444176650 1
a^2 + b^2 = m*p where m=
88555205325998957885745697878905775221348122914773300255530998859721472185840613932933
a^2 + b^2 = m*p where m=
```

```
42174891672093820681882820834470013918880145597580224365363798314598477184970273603 25
a^2 + b^2 = m*p where m=
1044376457714387421746815549989859052243110180542354519131764478700262185111802686272
a^2 + b^2 = m*p where m=434614370527443106698501831094899995257723150825985446315064353135188344250046881 17
a^2 + b^2 = m*p where m=33205825664498275695181063872238847747428106013951641644601348887645301496189432 5
a^2 + b^2 = m*p where m=75347396479820031770401108378067174082190485020270920267814328126195572215994196
a^2 + b^2 = m*p where m=25255750298552756441841143442605881654295828535730547977150097385192636617045
a^2 + b^2 = m*p where m=43700021515108738747855351218560188747874780107725874153258421074274307184 97
a^2 + b^2 = m*p where m=13646208131639058158102554458862289570303216195245016108695969708996211104 9
a^2 + b^2 = m*p where m=34589603475000815718567908189450795393721859295254557806452855146117125882
a^2 + b^2 = m*p where m=46880530916778128483172490072162241235508340054179223686963252750179228 13
a^2 + b^2 = m*p where m=14021897795738396336012920013243475474967710636738863169105322740875153 25
a^2 + b^2 = m*p where m=27570009806188124124562681704789992351250061693417038422439960064929401
a^2 + b^2 = m*p where m=87847752612444449420509180832535476189637273238578099010090404528131 41
a^2 + b^2 = m*p where m=16766075928286715018806065330616659512363252427131447049565772683808 29
a^2 + b^2 = m*p where m=19870650049370943899070080925480649207255875293292561663144471264174 5
a^2 + b^2 = m*p where m=25524414812237814199569128120295735842644202810319353046270759423698
a^2 + b^2 = m*p where m=27443387636133755256910265297074522638852094457260582283620096456 13
a^2 + b^2 = m*p where m=53503205368796632937005500700449482413892759790738500165939946932 0
a^2 + b^2 = m*p where m=10077727759094439994147448544713300941953032578100324770665067203 7
a^2 + b^2 = m*p where m=13746731255071704507216553390194917425777495895810184108517844138
a^2 + b^2 = m*p where m=76276782194106886230133886859850869121818321192469950765957024 1
a^2 + b^2 = m*p where m=20050362045748133383628750931059924923275269015474163198545521 7
a^2 + b^2 = m*p where m=49809004882010962796147645987222216151856813683370305244154888
a^2 + b^2 = m*p where m=88599480712176887680494858001878828948149836910648601114385 85
a^2 + b^2 = m*p where m=12943025367035934553290961832620321064534206231981606666179 7
a^2 + b^2 = m*p where m=81093641757319008436811706891904030269184036205339976547 70
a^2 + b^2 = m*p where m=31211151816747490760376128902587245612936629515779081169 61
a^2 + b^2 = m*p where m=62952439010563680877239074585070301749797223730683982844 5
a^2 + b^2 = m*p where m=57409634885228661489221526049090134500846394341571220436
a^2 + b^2 = m*p where m=20018838522334436101625900407873429510495315794510215797
a^2 + b^2 = m*p where m=16556790855123450534852938815986330347789253250341309 8
a^2 + b^2 = m*p where m=21463079975311904748336109277381699190252182769416601
a^2 + b^2 = m*p where m=32841904196278933319971194622192480205393905877378 57
a^2 + b^2 = m*p where m=10612947856272823012705781938295276511027061416060 02
a^2 + b^2 = m*p where m=55759054280564441297479420193780101713674527208753
```

```
a^2 + b^2 = m*p where m=339114682862671490820734545294265709628400545384 4
a^2 + b^2 = m*p where m=11586940939063816592771306695666675954550124683 81
a^2 + b^2 = m*p where m=34909553096678623019223298563248285153027100168 5
a^2 + b^2 = m*p where m=78092101010272264305432152437464155453172272026
a^2 + b^2 = m*p where m=15051101556005035622123971371008582307356548225
a^2 + b^2 = m*p where m=20555138241375443214216270198085228912047037 49
a^2 + b^2 = m*p where m=39581225304844891634192283849946102674355571 6
a^2 + b^2 = m*p where m=59553053103921967621656558756670840408880425
a^2 + b^2 = m*p where m=59146878338965305421822823044144381719186 73
a^2 + b^2 = m*p where m=76815051267770482703906459260393176835689 8
a^2 + b^2 = m*p where m=65416529072102282194391347229040032250673
a^2 + b^2 = m*p where m=71299274750523627219384748870293451821 70
a^2 + b^2 = m*p where m=92563315473279685523156944717371093901 7
a^2 + b^2 = m*p where m=16885212524429131967980400034018869885 8
a^2 + b^2 = m*p where m=54834828873695367093913329753845864545
a^2 + b^2 = m*p where m=10892650910333942023374707616255117122
a^2 + b^2 = m*p where m=58913441520754480595789067837815911 3
a^2 + b^2 = m*p where m=37538362891631237808493347200177737
a^2 + b^2 = m*p where m=69843454006035541153124634166893 49
a^2 + b^2 = m*p where m=29353943180403636191032142084816 0
a^2 + b^2 = m*p where m=83165627776212680329867857771501
a^2 + b^2 = m*p where m=21952464752510234910578664111620
a^2 + b^2 = m*p where m=20645223007220716547108718674 33
a^2 + b^2 = m*p where m=38656563891248047480429838341 7
a^2 + b^2 = m*p where m=26668268878099037214150008 74
a^2 + b^2 = m*p where m=54094506272272052239419728 9
a^2 + b^2 = m*p where m=83595900601971307523431466
a^2 + b^2 = m*p where m=36145253687778845380105
a^2 + b^2 = m*p where m=13932942047897980137165
a^2 + b^2 = m*p where m=98112375911585467445
a^2 + b^2 = m*p where m=14039461455225469121
a^2 + b^2 = m*p where m=2610566287160692853
a^2 + b^2 = m*p where m=467144899380242605
a^2 + b^2 = m*p where m=9801279552156625
a^2 + b^2 = m*p where m=244185215738218
a^2 + b^2 = m*p where m=12388698218789
```

```
a^2 + b^2 = m*p where m=3151808909053
a^2 + b^2 = m*p where m=780028469557
a^2 + b^2 = m*p where m=220894725805
a^2 + b^2 = m*p where m=23697853601
a^2 + b^2 = m*p where m=3230688757
a^2 + b^2 = m*p where m=841858265
a^2 + b^2 = m*p where m=45304001
a^2 + b^2 = m*p where m=9372457
a^2 + b^2 = m*p where m=1754145
a^2 + b^2 = m*p where m=428933
a^2 + b^2 = m*p where m=60146
a^2 + b^2 = m*p where m=2809
a^2 + b^2 = m*p where m=712
a^2 + b^2 = m*p where m=97
a^2 + b^2 = m*p where m=29
a^2 + b^2 = m*p where m=4
a^2 + b^2 = m*p where m=1
```

Check that $a^2 + b^2 = p$:

```
> a;
```

$$7766881905507050845172598218029833369440123277895 \quad (6$$

```
> b;
```

$$-9969792147013851944754165641884850918462852401638 \quad (7$$

```
> a^2+b^2;
```

$$10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000949 \quad (8$$

These values of a and b are unique up to sign changes, and interchanging a and b. With such a large prime p, we could not have found a and b by trial and error.